3-22-2019

Physical Layer Discrimination of Electronic Control Units Using Wired Signal Distinct Native Attribute (WS-DNDA)

Rahn M. Lassiter

PHYSICAL LAYER DISCRIMINATION OF ELECTRONIC CONTROL UNITS USING WIRED SIGNAL DISTINCT NATIVE ATTRIBUTE (WS-DNA) FINGERPRINTS

THESIS

Rahn M. Lassiter, Capt, USAF

AFIT-ENG-MS-19-M-038

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-19-M-038

PHYSICAL LAYER DISCRIMINATION OF ELECTRONIC CONTROL UNITS USING WIRED SIGNAL DISTINCT NATIVE ATTRIBUTE (WS-DNA) FINGERPRINTS

THESIS

Presented to the Faculty

Department of Electrical Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Rahn M. Lassiter, B.S.E.E.

Capt, USAF

21 March 2019

AFIT-ENG-MS-19-M-038

PHYSICAL LAYER DISCRIMINATION OF ELECTRONIC CONTROL UNITS USING WIRED SIGNAL DISTINCT NATIVE ATTRIBUTE (WS-DNA) FINGERPRINTS

THESIS

Rahn M. Lassiter, B.S.E.E.
Capt, USAF

Committee Membership:

Dr. Scott R. Graham
Chairman

Dr. Michael A. Temple
Member

Maj Timothy J. Carbino, PhD
Member

AFIT-ENG-MS-19-M-038

Abstract

The Controller Area Network (CAN) bus is a communication system used in automobiles to interconnect the electronic components required for critical vehicle operations. These components are called Electronic Control Units (ECU) and each one exercises one or more functions within the vehicle. ECUs can provide autonomous safety features and increased comfort to drivers but these advancements may come at the expense of compromised vehicle security. Researchers have shown that the standard automobile CAN bus can be hacked by 1) compromised *authorized* ECUs or 2) by *unauthorized* devices, or ECUs, that have been physically connected. Physical layer (PHY) device fingerprinting has emerged as one accepted approach to establishing vehicle security. This work investigates the application of AFIT's Wired Signal Distinct Native Attribute (WS-DNA) Fingerprinting using Multiple Discriminant Analysis Maximum Likelihood (MDA/ML) to achieve ECU discrimination. Demonstrations include 4-Class Cross Lot Discrimination (CLD) assessments with four Toyota Avalon ECUs with the same part number but different lot numbers as well as 9-Class Like Model Discrimination (LMD) assessments with nine Toyota Avalon ECUs of the same make and model as authorized devices. Rogue Arduino, Beagle Board, and CANable USB to CAN bus adapter are introduced and Rogue Reject Rate (RRR) estimated. Using WS-DNA features, RRR = 100% for rogue devices presenting false credentials for both the four class and nine class problem. Specific performance for compromised *authorized* ECU access attempts included 98% $\leq$ RRR $\leq$ 100% for the 4-class CLD assessment and 35.2% $\leq$ RRR $\leq$100% for the LMD assessment. Additionally, the Average Percent Correct Classification (%C) benchmark of %C = 90% was achieved for authorized devices at $SNR_{\Delta} \geq$ -8 dB for the 4-class CLD and at collected con-

ditions (SNR_{col}) for 9-class LMD assessments. Lastly, a pilot study was conducted using three CAN transceivers to study the effects of thermal cycling on statistical fingerprints and device discrimination. First-look discrimination results indicate that fingerprints do in fact vary with thermal cycling. Results for CAN transceiver thermal cycling include 1) classification in the range of 90% $\leq$ %C$\leq$ 100% for MDA/ML models trained at one temperature and tested at another and 2) post-thermal cycling features at a given temperature being different as the device temperature is cycled from low-to-high and high-to-low.

Acknowledgements

This has been one of the most challenging experiences of my life and I couldn't have accomplished this milestone without help. I want to thank God for good health throughout my time here. I want to thank my wife, kids, and family for all of their sacrifices and encouragement. I want to thank Dr. Graham, Maj Carbino, and Dr. Temple for being on my committee. Dr. Graham and Maj Carbino always had time to advise me as well as provide career and life advice. Dr. Temple always had 5 min (1 hour) to offer suggestions or help with problems along the way. I would like to thank the signals/comm professors for the beating me up in every class and giving me the skills I needed for this program. I would like to thank Nundu for explaining everything to me as well as teaching me proper English. I want to thank Steve Dunlap for his advice and assistance with my research as well as Ryan Gordon. Lastly, I want to thank my aunt for paving the way for me at AFIT.

Rahn M. Lassiter

Table of Contents

Page

Page

List of Figures

List of Tables

List of Abbreviations

Abbreviation		Page
ECU	Electronic Control Units	1
WS-DNA	Wired Signal Distinct Native Attribute	1
CAN	Controller Area Network	1
DARPA	Defense Advanced Research Projects Agency	2
CHT	CAN Hacking Tool	2
CCR	Center for Cyberspace Research	2
DNA	distinct native attributes	2
MSE	mean squared error	3
CMD	Cross Model Discrimination	3
CLD	Cross Lot Discrimination	3
LMD	Like Model Discrimination	3
AFIT	Air Force Institute of Technology	7
RF-DNA	Radio Frequency Distinct Native Attribute	7
MDA/ML	Multiple Discriminant Analysis Maximum Likelihood	7
SOF	Start of Frame	8
CRC	Cyclic Redundancy Check Field	8
EOF	End of Frame	8
DLC	Data Length Code	11
ACK	Acknowledgement	11
LIN	Local Interconnect Network	12
MOST	Media-oriented System Transport	12
MSE	mean squared error	15

Abbreviation		Page
CIDS	CAN Intrusion Detection System	15
ROC	Receiver Operating Characteristic	15
OBD-II	On Board Diagnostics	16
TD	Time Domain	16
PMF	Probability Mass Function	21
TVR	True Verification Rate	22
FVR	False Verification Rate	22
RRR	Rogue Rejection Rate	22
RAR	Rogue Acceptance Rate	22
CLD	Cross Lot Discrimination	25
SNR	Signal-to-Noise Ratio	33
RndF	Random Forest	71
GRLVQI	Generalized Relevance Learning Vector Quantization Improved	71
DRA	dimensional reduction analysis	71
SB-FSK	Slope-Based Frequency Shift Keying	71

Physical Layer Discrimination of Electronic Control Units Using WS-DNA Fingerprinting

I. Introduction

This research investigates the discrimination of Electronic Control Units (ECU) in automobiles via the signals that they transmit and provides a successful demonstration of the Wired Signal Distinct Native Attribute (WS-DNA) fingerprinting process. ECUs are electrical devices that work with mechanical components to control everything in an automobile from steering and braking to the windows and radio. The majority of ECUs required for driving operations are connected to the Controller Area Network (CAN) bus. The ability to achieve device identification and discrimination could be useful in detecting and even preventing unauthorized access on a network as well as identifying aging devices. This chapter provides an explanation of the operational and technical motivation for this research as well as research contribution, the methodology, the scope and assumptions, the research questions pursued, the support needed for this effort and the document organization.

1.1 Background

An overview of the operational and technical motivation for this research is provided in this section, as well as brief introduction into previous and related fingerprinting work.

1.1.1 Operational Motivation.

As automobiles become more technologically advanced and connected, they become more susceptible to hacking. In 2013, the Defense Advanced Research Projects Agency (DARPA) funded researchers to hack automobiles to expose security vulnerabilities [13]. Using a laptop connected to the Internet, the researchers were able to remotely turn off the engine, activate the windshield wipers and windshield wiper fluid, and even disable the brakes [13, 20]. Because most vehicles contain electronic controls and embedded systems on a network, this threat is not limited to automobiles but may extend to heavy vehicles, ships, and aircraft.

The technology needed to perform these types of attacks is becoming less complex and more accessible. In 2014, security researchers were able to develop a device called a CAN Hacking Tool (CHT) that costs less than $20 to make, is as small as an iPhone, and can be hooked up to a vehicle in as little as five minutes [31]. With this type of accessibility, the problem becomes more of a reality, not just for a high profile person, but for anyone driving a vehicle with computer controlled electronic components. The Center for Cyberspace Research (CCR) is currently investigating many methods for vehicle cyber security. WS-DNA can provide an additional layer of security and augment current security research for the CCR.

1.1.2 Technical Motivation.

Identification of rogue devices on a network may be achieved through various approaches. One approach is to examine the physical layer which consists of the signals that are transmitted on the CAN bus by the ECUs. Each ECU on the bus transmits packets, or bursts, of information and each burst that is transmitted has distinct native attributes (DNA) that are exclusive to the ECU that transmitted the burst; specifically the physical devices responsible for transmitting electrical signals. This

DNA is referred to as a fingerprint and previous research used fingerprinting as a way to discriminate between devices.

One researcher employed a correlation and mean squared error (MSE) approach to discriminating ECUs but the results were not considered adequate as better classification was achieved with a different approach and the fields used to extract statistical features are not feasible in a realistic CAN environment [8, 30]. More recent research has utilized neural net classifiers along with fingerprints to achieve device discrimination with one researcher achieving %C = 98% correct classification of devices [2]. However, all researchers did not use an actual ECU from a vehicle, rather they used the transceiver chip from an ECU coupled with a simulation board setup or developmental boards such as an Arduino Uno [2, 8].

This research explores a more realistic scenario by using production ECUs, in this case, Steering Angle Sensors (SAS) from a Toyota Avalon, and also using a machine learning algorithm to achieve device discrimination. Device discrimination is simply the ability to distinguish one device from another. This research considers both Cross Model Discrimination (CMD) (also referred to as Cross Lot Discrimination (CLD) in this document), defined here as devices with the same purpose or function on a vehicle but from different manufacturers or lots, and Like Model Discrimination (LMD), defined here as devices of the same model and manufacturer with different serial numbers. CMD can be thought of as distinguishing an iPhone from a Samsung while LMD can be thought of as distinguishing one iPhone from another iPhone. This thesis explored methods to achieve the maximum correct classification, i.e. correctly identifying a device by its unique characteristics when presented with a set of multiple fingerprints from different devices. Additionally, this thesis examined the effects of temperature variations on statistical fingerprints and device discrimination. Research contributions are identified in Table 1 as well as previous fingerprinting work. Not

identified in Table 1 is the fact that this research is the initial application of WS-DNA fingerprinting for ECUs.

1.1.3 Methodology - WS-DNA.

Using wired signals to generate fingerprints and achieve device discrimination is not a new process. The WS-DNA process used for this research was adopted from [3, 4, 5, 6, 25, 26, 27, 35, 36] and adapted for ECU application under consideration. Signals were collected from the output of each Steering Angle Sensor (SAS) using an oscilloscope and post-collection processing was accomplished using MATLAB®. The ECUs fingerprints were generated using a MATLAB® script that calculated the statistical features of a user selected Region of Interest (ROI). The ROI normally consists of a non-modulated burst such as a preamble, midamble or postamble [33]. The device fingerprints were compared to a set of training fingerprints and assessed to determine which training fingerprints the unknown fingerprints looked most like (classification) using a machine learning algorithm. Fingerprints were also compared to see how much one device looks like another device (verification) [33]. The two-part process of classification and verification is called device discrimination. The machine learning algorithm is given a portion of the known data to train on followed by a testing phase where the decisions of the algorithm are used for device classification and verification [33].

1.2 Research Questions

This section presents the research questions pursued in this work.

1. Which field or group of bits in a base frame format ECU can be used for CAN bus discrimination and which field or group of bits in a base frame format can be used to attempt to maximize ECU discrimination?

2. Is it possible to achieve better correct classification than previous researchers who used base frame format or extended frame format devices?

3. What type of effect does thermal cycling have on devices and on device discrimination?

4. How similar are unauthorized, or "rogue", devices such as the Arduino Uno or Beagle Board to authorized ECUs?

Table 1. Research contributions and previous DNA research

Technical Area	Previous Work		Current Research	
	Addressed	Ref #	Addressed	Ref #
TD Features	X	[23, 27, 34, 36, 35, 37, 40]	X	[25]
SD Features	X	[9, 10, 34, 40]		
GT Features	X	[33]		
CB Features	X	[4, 6]		
Correlation	X	[18, 19, 30]		
Emission Type				
Intentional	X	[21, 23, 27, 34, 36, 35, 37, 40]	X	[25]
Unintentional	X	[4, 6, 9, 10]		
Burst	X	[4, 6, 21, 23, 27, 34, 36, 37, 40]	X	[25]
Continuous	X	[9, 10]	X	[25]
Classification/Verification Process				
MDA/ML	X	[4, 6, 9, 10, 23, 27, 34, 36, 37, 40]	X	
GRLVQI	X	[23, 33, 34]		
RndF	X	[27]		
SVM	X	[8, 22]		
NN	X	[2, 4, 8, 22]		
Classification/Verification Devices				
Wireless Devices	X	[21, 23, 34, 36, 37, 40]		
Wired Devices	X	[2, 4, 7, 8, 22, 24, 27, 29, 36, 35]	X	[25]
Network Type				
CAN Bus	X	[2, 7, 8, 22, 24, 29]	X	
Device Type				
ECU	X	[7]	X	[25]
Thermal Effects				
CAN Transceiver			X	

1.3 Scope and Assumptions

Previous research examined how different cables and different cable lengths affected the fingerprints as well as affected the device discrimination [2]. This is a valid research effort to explore because different cable lengths and material induce different attenuation of the signal of interest, but this research is only be focused on ECU device discrimination. One key assumption in this research is that the ECU will behave the same as a standalone device as it would while connected to the controller area network. Another assumption is that all devices of interest for discrimination on the CAN bus will have the same invariant region containing the same bits and bit transitions. In this case, devices with different identification numbers should be base frame format and transmit the same number of data bits.

1.4 Support

The following items were necessary to accomplish signal collection and post collection processing:

- 10 ea Toyota Steering Angle Sensors
- Oscilloscope
- Computer with MATLAB®
- Ardunio Uno with Seeed CAN shield
- Beagle Board
- CANable USB to CAN adapter
- 3 ea ISO 1050 CAN transceivers

Funding for this research was provided by CCR at the Air Force Institute of Technology (AFIT). Experimental support needed for this research was provided by CCR contractors.

1.5 Document Organization

The remainder of this thesis document is outlined in this section. Chapter 2 reviews applicable literature related to CAN bus, ECU, device identification and device discrimination. Chapter 3 provides a detailed explanation of the research methodology to include Radio Frequency Distinct Native Attribute (RF-DNA) fingerprinting as well as WS-DNA. It also includes an explanation of signal collection, post-collection processing using the Multiple Discriminant Analysis Maximum Likelihood (MDA/ML) classification and verification machine learning algorithms. Chapter 4 includes an explanation of the MDA/ML classification and verification results and analysis. Chapter 5 offers conclusions based on the results in Chapter 4 and identifies relevant future work.

II. Literature Review

2.1 Introduction

Chapter 2 provides an overview of the system under test as well as a background of research methodology used in Chapter 3. This chapter also covers security vulnerabilities associated with the Controller Area Network (CAN) bus and Electronic Control Units (ECU) as well as previous research to identify or fingerprint devices. A background on thermal effects on vehicles is also presented. Section 2.2 provides an overview of the CAN bus with details on the frame formats, the fields, the signal characteristics, and the equipment used to create rogue devices. Section 2.2 is necessary to understand the best field or group of bits to identify an ECU based on its signal characteristics. Section 2.3 provides an overview of some of the security vulnerabilities of the CAN bus and ECUs and Section 2.4 provides an overview of previous research methodologies related to the security issues associated with the CAN bus. The last section provides a detailed explanation of Radio Frequency-Distinct Native Attribute (RF-DNA) as well as Wired Signal-Distinct Native Attribute (WS-DNA) which utilizes the same techniques as RF-DNA. This section also provides as explanation of the process of device classification which is achieved via Multiple Discriminant Analysis Maximum Likelihood (MDA/ML). Lastly, this section provides an overview of Device Verification which covers authorized and rogue device acceptance and rejection.

2.2 Controller Area Network (CAN) Bus

This section provides a brief history of the CAN bus, an overview of the different message formats, and a description of each field in a CAN message which includes the Start of Frame (SOF), the Arbitration Field, the Control Field, the Data Field, the Cyclic Redundancy Check Field (CRC), and the End of Frame (EOF). Additionally,

this section covers the concept of stuff bits, additional networks in a vehicle, and an overview of how bits are generated in the physical layer of a vehicle.

2.2.1 History.

CAN Bus is a communication system that was created in the 1980s by Bosch GmbH to simplify wiring in automobiles [12]. The controller area network is comprised of many different devices called Electronic Control Units (ECU) which transmit and receive critical information across the network such as vehicle speed, engine RPM, and the angle of the steering wheel. The CAN 2.0 standard is the latest version that is used on vehicles and transmits data up to 1 Mbps. Figure 1 illustrates the different networks that are inside a technologically advanced vehicle. The figure is used to show that all of the ECUs that are critical to physically driving the vehicle are located on the CAN bus. The CAN bus has two message formats which are the base frame and the extended frame formats.

2.2.2 Frame Formats.

The CAN bus employs two types of message formats: base and extended frame formats. The difference between base and extended is that extended frame format has two identification, or arbitration, fields. Extended frame also contains a few more bits that are not relevant to this research. The research will focus on the base frame format which is shown in Figure 2. This figure illustrates a typical base frame which includes the Arbitration Field, the Control Field, the CRC Field, and the End of Frame [12].

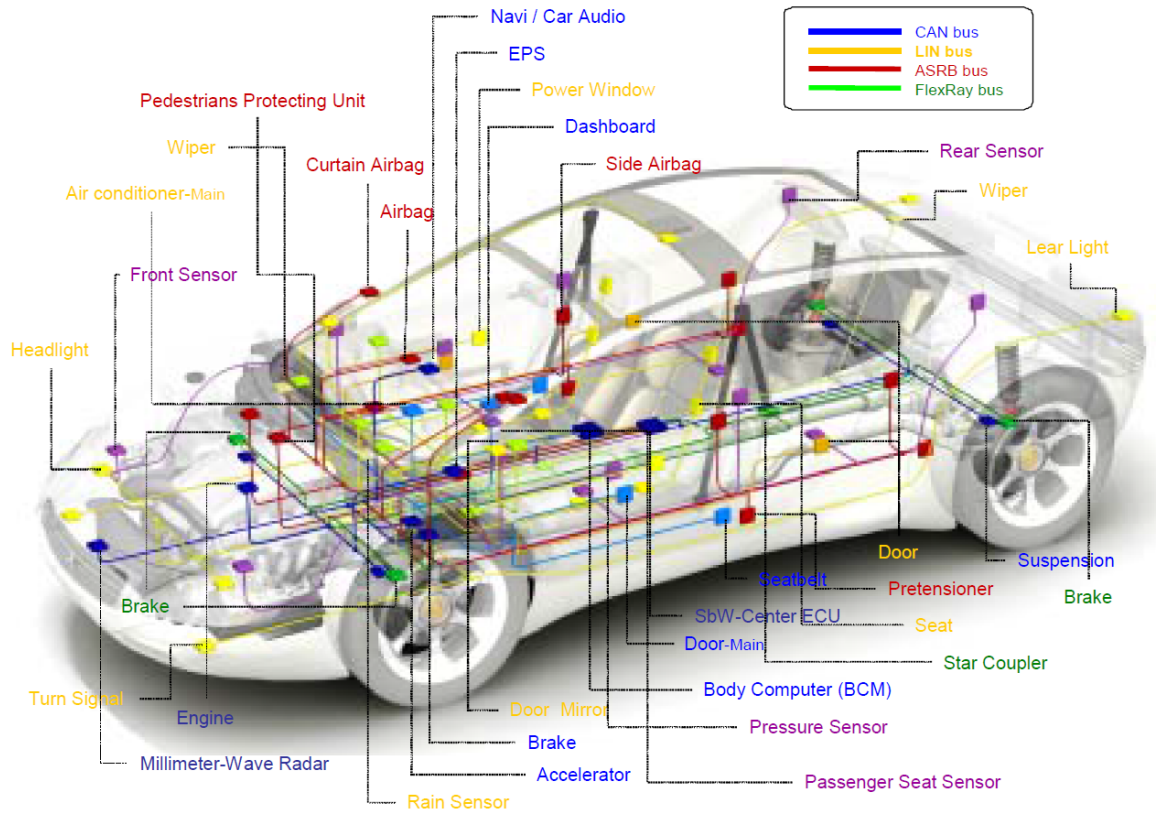

Figure 1. Various networks inside of a technologically advanced vehicle [31].

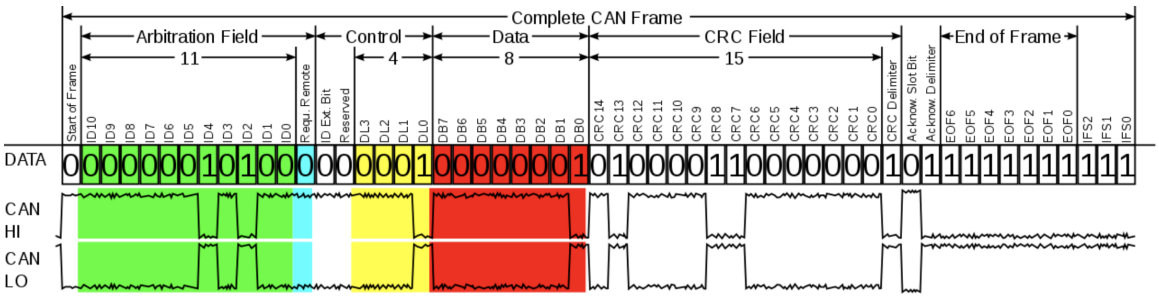

Figure 2. Breakdown of complete CAN frame, or message, from an ECU [16].

2.2.3 Start of Frame.

The Arbitration Field is preceded by the Start of Frame (SOF) bit which signifies that an ECU is about to transmit information and the SOF is always a dominant bit. The Arbitration Field is composed of an 11 bit identifier that signifies which ECU on the network is transmitting and establishes the priority of the ECU on the

bus. Since any ECU can transmit at any time, the arbitration is based on the highest priority message. The ECU with the lower identifier number has the highest priority and wins the arbitration. The arbitration protocol is used when more than one ECU is transmitting at the same time, also called a collision, and an example of how arbitration works on the CAN bus is shown in Figure 3 [12].

2.2.4 Control Field.

The Control Field is comprised of the ID extension bit and a Reserved bit which are always dominant bits. These bits are followed by the Data Length Code (DLC) which determines how many bits will be transmitted in the data field.

2.2.5 Data Field.

The Data Field is comprised of zero to 64 bits of information and is the field that contains the message that is broadcast to all ECUs on the CAN bus. The bits transmitted in this field vary from message to message [12].

2.2.6 Cyclic Redundancy Check Field.

The CRC Field is a 15 bit field intended to preserve the integrity of the data that was transmitted. The bits in this field are generated based on the bits that are transmitted in the data field. Following the CRC are the CRC delimiter, the Acknowledgement (ACK) slot, and the ACK delimiter. These bits are always transmitted as

	SOF	Identifier						
ECU 1	0	0	0	0	1	0	1	0
ECU 2	0	0	0	1	stops transmitting			
CAN Bus	0	0	0	0	1	0	1	0

Figure 3. An example of how arbitration works on the CAN bus. ECU 1 has a lower binary value identification than ECU 2 which means that it wins the arbitration and continues to transmit.

recessive bits [12].

2.2.7 End of Frame.

The End of Frame consists of seven consecutive recessive bits that signify the end of transmission for an ECU. The EOF is the only field that can transmit more than five consecutive identical bits. If more than five consecutive recessive bits are transmitted in another field, an error occurs on the CAN bus. Following the EOF are the Interframe Spacing bits. There are at least three consecutive recessive bits which represent the idle time on the CAN bus between messages and allows for SOF synchronization [12].

2.2.8 Stuff Bits.

Stuff bits are bits that are automatically injected into a frame from the sender when more than five consecutive ones or five consecutive zeros are sent both to ensure synchronization and to let the receiver know that an error is not present in the field or message [12]. The total number of bits transmitted increases based on the number of stuff bits added.

2.2.9 Additional Networks.

There are additional networks that exist on vehicles now such as the Local Interconnect Network (LIN) and the Media-oriented System Transport (MOST). These networks also provide access for an attack but are not included in this research [2].

2.2.10 Physical Layer.

The CAN transceiver is a device within an ECU that converts bits (ones and zeros) into CAN logical signals which are called CAN-Hi and CAN-Lo. The CAN-

Hi and CAN-Lo outputs work on a Non Return to Zero (NRZ) differential voltage protocol. The CAN-Hi and CAN-Lo output voltages are 2.5 volts when the ECU is idle or transmitting a one, but the CAN-Hi voltage is increased to 3.5 volts and the CAN-Lo is decreased to 1.5 volts when a zero is being transmitted. The difference between the voltage outputs is then approximately 2 volts and represents a logical 0, whereas when both CAN-Hi and CAN-Lo are 2.5 volts, the difference is zero volts which represents a logical 1 [12]. An example of the differential voltage is shown in Figure 2.

2.2.11 Rogue Devices.

The rogue devices used for this research are devices that are commonly used to emulate ECUs as well as simulate a CAN bus. The first rogue device was an Arduino Uno with a Seeed CAN shield. The Arduino Uno is a development board that uses a ATmega328 microcontroller and has a wide range of applications including simulating ECUs. This device was used in previous research to simulate ECUs for device discrimination [2, 1, 8]. The second rogue device was a Beagle Board development board called BeagleBone Black which utilized a locally manufactured shield coupled with an IS0 1050 CAN transceiver. The BeagleBone uses an Arm Cortex processor and also has a wide range of applications including ECU simulation [11]. The IS0 1050 CAN transceiver is an eight pin Texas Instrument chip that has a wide range of applications from transportation, HVAC, medical, etc [38]. The transceiver can send data up to 1 MBPS and is rated for ambient temperature operation from -55 °C to 105 °C [38]. The last device used was a CANable USB to CAN adapter. The CANable is a device that can be connected to a CAN bus to monitor message traffic but it can also be programmed to act as an ECU and send messages at speeds of up to 1 MBPS [17].

2.3 Security Vulnerabilities

CAN bus vulnerability has been considered by several groups, including researchers at the University of Washington (UW) as well as by security researchers Miller and Valasek. UW researchers were able to prove that a vehicle can be hacked wirelessly through access points such as On-Star. Miller and Valasek initially hacked an automobile via physical access to the dashboard but were also able to remotely hack an automobile and do things such as turn on the windshield wipers and windshield wiper fluid, activate the brakes, and disable the engine [13, 20, 14].

Additional technology such as the CAN Hacking Tool (CHT) exists that utilizes physical access within a vehicle to give hackers remote access [31]. Physical access can provide the ability for hackers to remotely control the vehicle as seen in [13]. As previously mentioned, these devices can be created for as little as $20, making these devices very accessible.

2.3.1 Thermal Effects.

Automobiles, and therefore ECUs, experience a wide range of temperature variations throughout their life cycles from normal weather patterns and operation of the vehicle. In a study of temperature variations in parked vehicles, it was found that the cabin temperature and trunk temperature experience much higher temperature variations compared to the outside air temperature fluctuations. During a nine day experiment, although air temperature varied approximately 15 °C, the trunk temperature experienced an approximately 20 °C change and the cabin temperature experienced as much as 40 °C variations [15].

2.4 Related Work

There have been various methodologies employed to create intrusion detection systems or establish security on a CAN bus. The review of related work is limited to previous methods to fingerprint ECUs in order to identify rogue or malfunctioning devices [2, 7, 8, 22, 30]. Early attempts at ECU classification or discrimination employed a mean squared error (MSE) and convolution approach. The MSE approach used the fingerprints as the reference data or training data and compared a new set of unknown fingerprints to the reference fingerprint. A low MSE value means that the unknown fingerprints are similar to a set of reference fingerprints and a high MSE value means that the unknown fingerprints are not similar to the reference fingerprints. For the convolution approach, the reference fingerprints were convolved with each set of unknown fingerprints. The maximum value of the convolution was used to determine "signal similitude" which appears to mean that the method is similar to correlation. The results according to the confusion matrices indicate that they achieved correct classification of $90 \leq \%C \leq 100\%$ [30].

A vastly different approach was used by [7] which involved using the internal clock of ECUs to identify the transmitting ECU. Fingerprints for this method were generated by using the clock offset, the clock frequency, and the clock skew. The researchers created fingerprints based on these variables and used a recursive least squares algorithm to model the behavior of the clocks of each ECU. A device called the CAN Intrusion Detection System (CIDS) was developed to install within a vehicle to detect malicious activity. CIDS uses a correlation between clock offsets in received messages to identify ECUs. The methods used by these researchers produced a minimum of approximately 97% probability of detection with a maximum of approximately 40% probability of false alarm according to the Receiver Operating Characteristic (ROC) curve presented. These metrics are similar to RF-DNA verification metrics which are

covered in the next section.

The majority of the fingerprinting methodologies used the statistical properties of a signal together with machine learning or neural net classifiers to identify unique attributes within the extracted features [2, 8, 22]. [2] used a CAN transceiver and development board setup to simulate the CAN bus and ECU, [8] utilized CAN Boards connected on a physical network to simulate various ECUs and the CAN bus while [22] plugged a device directly into the On Board Diagnostics (OBD-II) port on a vehicle to accomplish signal acquisition. The three different methods of signal collection coupled with similar methods of fingerprint generation and neural network classifiers produced a maximum correct classification of %C = 98.6% , %C= 96.5%, and %C = 86% respectively [2, 8, 22].

2.5 Radio Frequency Distinct Native Attribute (RF-DNA)

Radio Frequency Distinct Native Attribute (RF-DNA) is a device discrimination and classification methodology developed by AFIT to aid in detection of rogue devices, identification of aging devices, or augmentation of bit level security [3, 33, 36, 40]. Signals are collected intentionally and unintentionally from the RF emissions of devices. Distinct Native Attribute (DNA) fingerprints of the emissions are generated by looking at the statistical features of the amplitude, frequency or phase of the signals [3, 9, 28, 26, 33, 36, 39].

2.5.1 Time Domain (TD) Fingerprinting.

Time Domain (TD) Radio Frequency fingerprints are generated by utilizing the instantaneous responses of a signal which include the Instantaneous Amplitude (IA), the Instantaneous Frequency (IF) and the Instantaneous Phase (IP). A real valued signal must be broken up into I-Q samples via the Hilbert Transform [3] which for a

discrete real valued signal, $s(k)$, produces $s(k) = s_Q(k) + s_I(k)$ where the amplitude $a(k)$, the frequency $f(k)$ and the phase $\phi(k)$ are calculated by

$$a(k) = \sqrt{s^2(k)}, \tag{1}$$

$$\phi(k) = \tan^{-1}\left[\frac{s_Q(k)}{s_I(k)}\right], \tag{2}$$

$$f(k) = \frac{1}{2\pi}\left[\frac{d\phi(k)}{dk}\right]. \tag{3}$$

The TD features are normalized and centered by subtracting the mean of the respective feature and dividing the total by the maximum value of the respective feature. The equations for these normalized features are

$$\overline{a}_c(k) = \frac{a(k) - \mu(a)}{\max\limits_{\mathrm{k}} a_c(k)}, \tag{4}$$

$$\overline{\phi}_c(k) = \frac{\phi(k) - \mu(\phi)}{\max\limits_{\mathrm{k}} \phi_c(k)}, \tag{5}$$

$$\overline{f}_c(k) = \frac{f(k) - \mu(f)}{\max\limits_{\mathrm{k}} f_c(k)}. \tag{6}$$

The ROI is divided into equal subregions, N_R, and typically the ROI is included as a subregion to produce a total of $N_R + 1$ subregions for statistical feature extraction [3]. The typical features that are extracted include standard deviation (σ), variance (σ^2), skewness (γ) and kurtosis (κ). These statistics are calculated for a subregion to generate one fingerprint F_{RF_i}. Each regions fingerprints are concatenated to form the composite fingerprint F_{RF}. The fingerprints can be represented by the following

equations

$$F_{RF_i}^{RF} = [\sigma_{R_i}, \sigma_{R_i}^2, \gamma_{R_i}, \kappa_{R_i}]_{1\times 4}, \tag{7}$$

$$F_{a,\phi,f}^{RF} = [F_{R_1}^{RF} : F_{R_2}^{RF} : F_{R_3}^{RF} : \cdots : F_{R_{N+1}}^{RF}]_{1\times[4(N_R+1)]}, \tag{8}$$

$$F_{C}^{RF} = [F_{a}^{RF} : F_{\phi}^{RF} : F_{f}^{RF}]. \tag{9}$$

The features that are included in an RF-DNA fingerprint are made up of the number of responses, N_{resp}, the number of statistical features, N_{stat}, and the number of subregions, N_R. For example, if $N_{resp} = 12$, $N_{stat} = 3$ and $N_R = 9$ then the number of features $N_{feat} = 12 \times 3 \times 9 = 324$ features [3]. An example of the regional and composite fingerprint generation process is shown in Figure 4.

2.5.2 MDA/ML.

Device fingerprints are compared using a classifier called Multiple Discriminant Analysis Maximum Likelihood (MDA/ML). Multiple Discriminant Analysis is a dimensionality reducing algorithm that takes the extracted features, or fingerprints, and reduces them to $N_C = N_D$-1 classes, where N_D is the number of devices. The

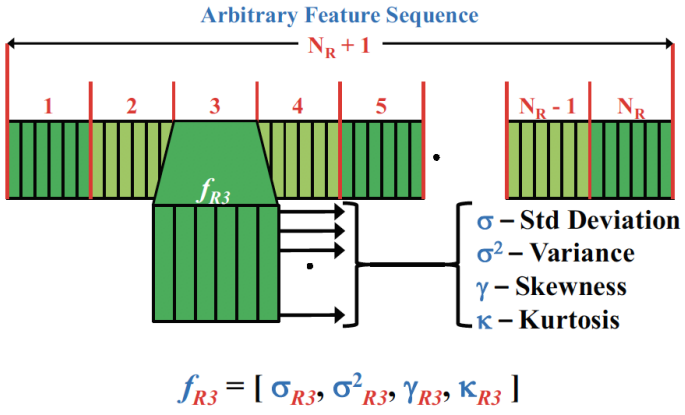

Figure 4. Example of feature extraction used to generate fingerprints for RF-DNA [3].

maximum likelihood classifier is based on an assumption that the data has a Gaussian distribution and assumes equal priors and uniform costs. The classifier compares each testing fingerprint to every set of training fingerprints available to make a classification decision [33].

2.5.3 Multiple Discriminant Analysis (MDA).

MDA is an extension of Fischer's Linear Discriminant analysis that uses N_D-1 classes instead of two classes [33]. The primary purpose of MDA within the RF-DNA methodology is to decrease the intra-class variance and increase the inter-class means. Accomplishing this is done by calculating the scatter matrices of the inter-class means using

$$S_b = \sum_{i=1}^{C} P_i \Sigma_i \tag{10}$$

as well as calculating the intra-class variances using

$$S_w = \sum_{i=1}^{C} P_i (\mu_i - \mu_0)(\mu_i - \mu_0)^T \tag{11}$$

where C is the number of classes, P_i is the prior probability of the class c_i, and Σ_i is the covariance matrix [3]. These calculations are based on the assumption of equal costs and equal prior probabilities which means that the cost for incorrectly classifying ECU_1 is the same cost as incorrectly classifying ECU_N. Equal prior probabilities means that the probability that ECU_1 is present is the same as the probability that ECU_N is present. Equations 10 and 11 are used to create a projection matrix W. The eigenvectors that produce W_{best}, the best combination of minimized intra-class spread versus maximized inter-class mean distance, are used along with the mean vector μ^W and the covariance matrix Σ^W to classify fingerprints within the Maximum Likelihood

process [3, 36].

2.5.4 Maximum Likelihood.

The ML estimator is based on the Bayesian posterior probability and the assumption that the data has equal prior probabilities as well as uniform costs. The estimator is also based on the assumption that the data is normally distributed. An unknown fingerprint F is assigned to class c_i where i ranges from 1 to the number of classes, N_c. The conditional probability $P(c_i|F)$ is the probability that the unknown fingerprint belongs to c_i. The Bayes' probability is then calculated using

$$P(c_i|F) = \frac{P(F|c_i)P(c_i)}{P(F)} \tag{12}$$

where $P(c_i)$ is the probability that class c_i is present and $P(F)$ is the probability that the fingerprint F is present. Since we assume equal priors, $P(c_i)$ and $P(F)$ are constants and remain the same regardless of class or fingerprint. Because they are constant, these terms can be ignored, reducing Equation 12 to

$$P(c_i|F) = P(F|c_i). \tag{13}$$

The value for the remaining probability is calculated using the multivariate Gaussian equation

$$P(F|c_i) = \frac{1}{2\pi^{\frac{N_c-1}{2}}\sqrt{|\Sigma^W|}} exp\frac{-1}{2}(F-\mu_i)^T(\Sigma^W)^{-1}(F-\mu_i). \tag{14}$$

The results of this equation produce the values that are used to determine the correct classification percentage which is the number of correctly identified testing fingerprints divided by the total number of fingerprints available.

2.5.5 Wired Signal Distinct Native Attribute Fingerprints.

Wired Signal Distinct Native Attribute (WS-DNA) Fingerprinting is an extension of RF-DNA that uses the same methodology to generate fingerprints and for device classification and verification. The only difference between RF-DNA and WS-DNA is the method used for signal acquisition. WS-DNA signals are collected from the wires of a device whereas RF-DNA signals are collected from the RF emissions transmitted in the environment. One advantage that WS-DNA has over RF-DNA is that the signal-to-noise ratio (SNR) of the collected signals is typically higher than the signals collected using RF receivers [36].

2.5.6 Cross Validation.

A K-Fold cross validation process is also used to increase the reliability of the MDA/ML classifier. First, this process partitions the data into K equal parts. Then, one of the blocks is held out and K-1 blocks are used for training and the block that is held out is used for testing. This process is repeated until all K blocks are held out and tested. The projection matrix that produces W_{best}, the projection matrix that was previously explained in Section 2.5.2, is then used in the MDA/ML process for testing [3].

2.5.7 Device ID Verification.

Device verification is achieved by comparing one set of fingerprints to another set of fingerprints to assess how similar the devices are. During the verification process, a measure of similarity is chosen. From this measure of similarity, a test statistic Z_V is established. From this test statistic, a Probability Mass Function (PMF) is generated and a decision threshold $t_V(d)$ is established. This threshold is established based on the user selected acceptance and rejection rates during the training phase

of verification. During testing, an unknown set of fingerprints are presented and test statistics are generated. The test statistics are compared to the threshold $t_V(d)$ and the device is either accepted (rightly or wrongly) or rejected (rightly or wrongly) [3]. The intent is to observe how much a device looks like itself or others in an attempt to detect rogue devices attempting to mimic authorized devices. An error occurs when an authorized device is rejected and when a rogue device is accepted. Results from the verification process are presented as

- True Verification Rate (TVR)- The percentage of authorized device attempts accepted as an authorized device over the total number of attempts
- False Verification Rate (FVR) - The percentage of rogue device attempts accepted as an authorized device over the total number of attempts
- Rogue Rejection Rate (RRR) - Total number of rogue attempts rejected versus total number of attempts
- Rogue Acceptance Rate (RAR) - Total number of rogue attempts accepted versus the total number of rogue attempts

and graphically will be shown on a Receiver Operating Characteristic (ROC) curve.

Table 2. Output of Verification Process

	Authorized	Rogue
Authorized	Accept (Correctly) TVR	Reject (Incorrectly) FVR
Rogue	Accept (Incorrectly) RAR	Reject (Correctly) RRR

2.6 Conclusion

Based on the literature review of [2, 8, 22], extracting the statistical features of a signal coupled with using a machine learning or neural network approach are the best methods to achieve greater than 90% device discrimination. While the general methods of [2, 8, 22] are understood, the exact details of the statistical features used are somewhat vague. The process for statistical feature extraction is very clear in [3, 9, 28, 33, 36, 39] and the process of WS-DNA has not been applied to ECUs on a CAN bus. WS-DNA was used because it offers a very clear methodology and served as an equivalent comparison to the methods used and results achieved by [2, 8, 22]. Details on the methodology for WS-DNA are presented in Chapter 3.

III. Methodology

Chapter 3 provides a detailed explanation of the implementation of the Wired Signal Distinct Native Attribute (WS-DNA) methodology presented in Chapter 2. Section 3.1 presents the device under test for this research and Section 3.2 presents the experimental hardware setup and collection process. Section 3.3 provides the thermal cycling methodology. Section 3.4 presents the signal Burst Extraction methodology and Section 3.5 details the Region of Interest (ROI) selection and the subregion selection. Section 3.5 explains the pre-fingerprint generation filter type and filter bandwidth selection. Lastly, Section 3.6 presents the Multiple Discriminant Analysis Maximum Likelihood (MDA/ML) parameters that were used for device classification and verification as well as provides examples of MDA/ML results.

3.1 Device Under Test

The Device Under Test (DUT) for this research was a Toyota Avalon Steering Angle Sensor (SAS) and is pictured in Figure 5. The SAS is a device mounted in the steering column of the vehicle and reports the current angle of the steering wheel. This sensor is especially important in vehicles that use autonomous parking and will likely be one of the more important devices in self-driving vehicles. The components identified in Figure 5 were designated the Control Unit and the CAN Transceiver (CAN TRx) and are highlighted here because they may be the subcomponents responsible for variations in the signals. The first two digits of the Control Unit appear to correspond to the year that the component was manufactured. SAS 0 and SAS 11 were both obtained from used vehicles and SAS 1 - SAS 10 were all unused devices. The SAS that was used for this research transmits data at $f_{SAS} = 500$ kHz and each frame, if uninterrupted, transmits approximately every 260 μs. To accomplish the

Like-Model Discrimination (LMD) assessment, a total of $N_C = 9$ classes of the same part number and same lot number were used and $N_C = 4$ classes of different lot numbers but the same part number were used for Cross Lot Discrimination (CLD). Device details are shown in Table 3 and 4 which include the average collected SNR (SNR_C) for all devices.

3.2 Experimental Hardware Setup

This section covers the hardware and hardware settings used in SAS signal collection. The signals were extracted using a KeySight InfiniiVision MSOX3054T 5.0 GHz Oscilloscope. The SAS works on a differential voltage and requires two probes to cap-

Table 3. Devices Under Test in $N_C = 4$ Class Cross Lot Discrimination

Lot	Device	ID	Avg SNR_C	Control Unit	CAN TRx
503G	1	SAS 0	42.9 dB	1535 E05	5G3 60G4
823F	2	SAS 1	42.4 dB	1736 E06	7K2 60C8
826I	3	SAS 2	43.5 dB	1802 E03	8B4 613X
523E	4	SAS 11	43.4 dB	1531 E12	5G3 60E7
		Avg	**43.1 dB**		

Table 4. Devices Under Test in $N_C = 9$ Class Like Model Discrimination

Lot	Device	ID	Avg SNR_C	Control Unit	CAN TRx
823F	1	SAS 1	42.4 dB	1736 E06	7K2 60C8
823F	2	SAS 3	43.0 dB	1736 E08	7K2 60C8
823F	3	SAS 4	42.6 dB	1736 E08	7K2 60C8
823F	4	SAS 5	42.9 dB	1736 E06	7K2 60C8
823F	5	SAS 6	42.8 dB	1736 E06	7K2 60C8
823F	6	SAS 7	42.7 dB	1736 E06	7K2 60C8
823F	7	SAS 8	42.7 dB	1736 E08	7K2 60C8
823F	8	SAS 9	43.1 dB	1736 E06	7K2 60C8
823F	9	SAS 10	42.7 dB	1736 E08	7K2 60C8
		Avg	**42.8 dB**		

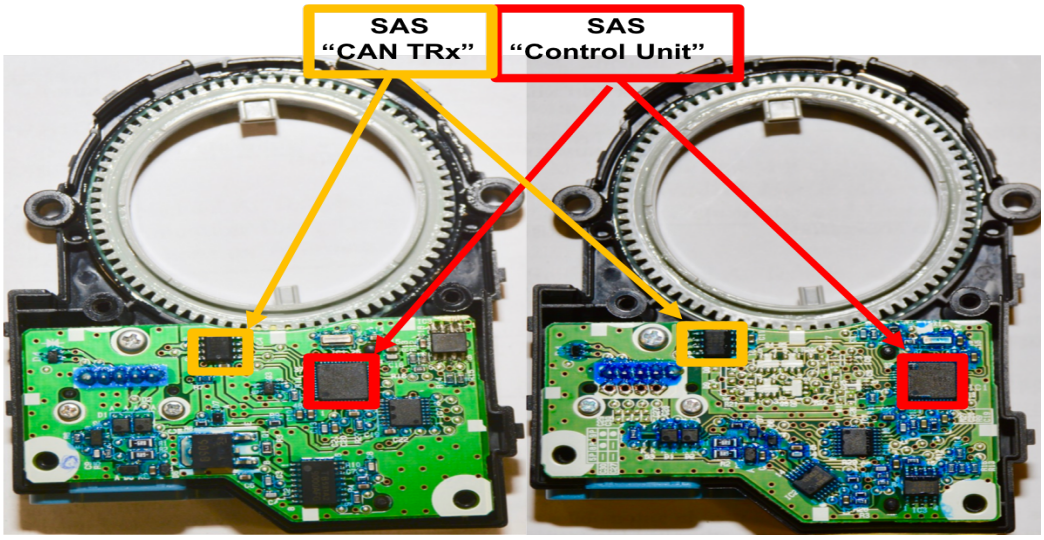

Figure 5. Internal View of Toyota Avalon Steering Angle Sensor (SAS). The ”Control Unit” and ”CAN Transceiver” are identified for both the older (left) and newer (right) SAS.

ture both the CAN-Hi and the CAN-Lo signals. The oscilloscope settings used were a sample rate of $fs = 1$ GSamp/Sec (GSPS), a horizontal scale of 30 ms/div, a vertical offset of 0 volts, and a vertical scale of 1 volt/div. To reduce environmental and collection bias, a random permutation of five collections of $N_{bursts} = 200$ bursts for each device were taken over a one week period at various times and various temperatures as shown in Table 5. All recorded temperatures are in Fahrenheit (F) and were obtained from a thermostat in the CCR lab. To further reduce experimental variability, each SAS was locked into the same position so that all devices transmitted the same 64 bit message and all devices were powered using the same power supply.

3.3 Thermal Cycling

This section details the methods used to thermally cycle the CAN transceivers which uses the same setup as Rogue Device 2 with 3 different transceivers used for this assessment. Thermal cycling was accomplished using two different methods; in Case 1, the CAN transceiver was 1) at ambient temperature, 2) cooled to approxi-

Table 5. Random permutation of SAS collections

SAS	Date/Time	Temp	SAS	Date/Time	Temp	SAS	Date/Time	Temp	SAS	Date/Time	Temp	SAS	Date/Time	Temp
8	9/11 0925	74	11	9/12 0908	74	9	9/13 0920	74	1	9/14 1009	74	4	9/17 1219	74
2	9/11 1005	74	3	9/12 0950	74	7	9/13 1002	74	3	9/14 1118	74	7	9/17 1258	74
3	9/11 1048	74	10	9/12 1031	74	0	9/13 1044	74	9	9/14 1159	73	1	9/17 1339	74
1	9/11 1131	73	8	9/12 1117	74	1	9/13 1126	74	5	9/14 1243	74	5	9/17 1442	75
5	9/11 1210	73	4	9/12 1200	74	6	9/13 1208	74	10	9/14 1333	73	9	9/17 1523	74
6	9/11 1253	73	1	9/12 1241	74	3	9/13 1256	74	8	9/14 1503	73	2	9/17 1603	74
4	9/11 1334	74	0	9/12 1322	75	10	9/13 1339	74	4	9/14 1415	73	8	9/17 1644	74
10	9/11 1437	74	6	9/12 1423	74	5	9/13 1447	74	11	9/14 1626	74	10	9/17 1727	74
9	9/11 1519	74	7	9/12 1505	74	4	9/13 1630	74	7	9/14 1709	73	3	9/18 0737	74
11	9/11 1600	74	9	9/12 1547	73	2	9/13 1713	74	0	9/17 1007	74	11	9/18 0940	74
7	9/11 1642	74	2	9/12 1629	74	8	9/14 0730	74	2	9/17 1058	74	0	9/18 1025	73
0	9/11 1722	74	5	9/12 1716	74	11	9/14 0927	74	6	9/17 1138	74	6	9/18 1108	74

mately 0 °C, 3) heated back to ambient, 4) heated to 50 °C from ambient, 5) heated to 75 °C from 50 °C, 6) cooled to ambient from 75 °C. Ambient temperature for these assessments are ≈ 25 °C. These collections are illustrated in Figure 6. Devices were heated using a Watlow oven and cooled using a common refrigerator operating at a temperature of approximately 0 °C. Additionally, devices were cooled or heated to ambient temperature by placing them in the CCR lab. Each of the first five collections involved a 30 minute operating time as well as a 30 minute dwell time at each

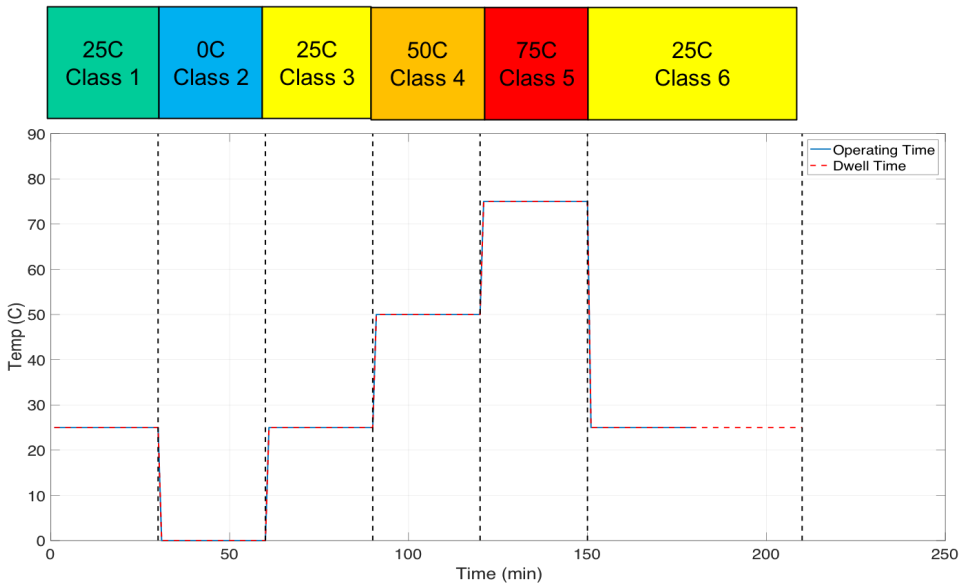

Figure 6. Dwell time, Operating time, and temperature for each of the $N_C = 6$ classes used for Case 1 thermal cycling.

temperature before collections were made. This was done in an attempt to prevent thermal shock to the transceivers. Class 6 was collected after one hour of dwell time at ambient temperature to allow the temperature to gradually drop from 75 °C to approximately 25 °C. This class was also collected after a 30 minute operating time which was used for all classes in order to reach a steady state operation.

For Case 2 thermal cycling, all $N_C = 3$ classes were collected at ambient temperature. Class 1 was collected before heating the CAN transceiver while operating in ambient temperature conditions. Class 2 was collected after the device was heated from ambient temperature to 50 °C and cooled to ambient temperature as shown in Figure 7. Class 3 was collected 24 hours after Class 2 while remaining in a temperature controlled environment at ambient temperature. Each of the three classes was created by collecting $N_{bursts} = 200$ bursts five different times between 1600-1700 on three consecutive days.

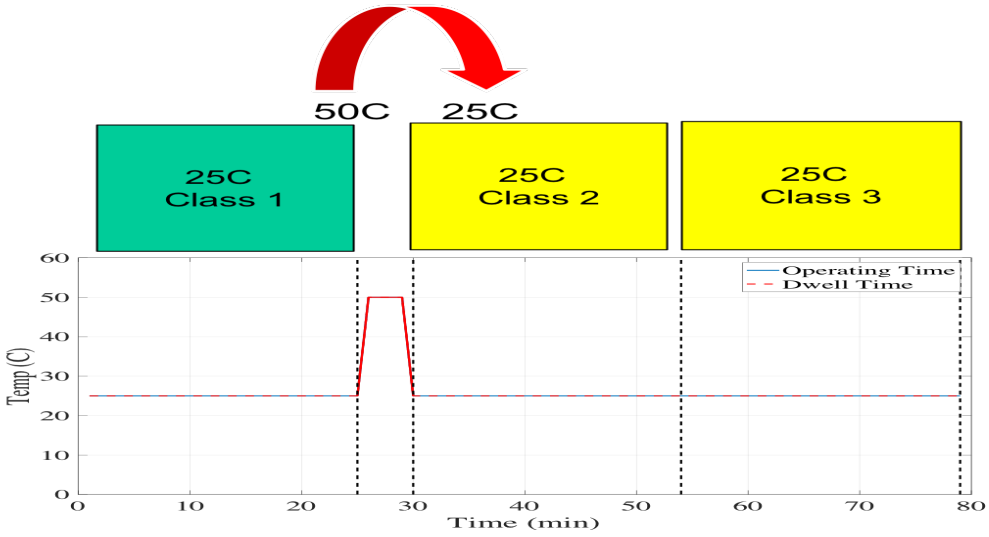

Figure 7. Dwell time, Operating time, and temperature for each of the $N_C = 3$ classes used for Case 2 thermal cycling.

3.4 Post-Collection Processing

This section provides the details for processing the extracted SAS signals using MATLAB® which includes the ROI used for WS-DNA, filter selection, SNR scaling, and SNR estimation.

3.4.1 Digital Filter.

This section covers the filter used to reduce additive noise before generating fingerprints. The filter was generated using $N_B = 2$ and the MATLAB® *filtfilt* function resulting in a 4th order baseband Butterworth filter with a bandwidth $W_{BB} = 500$ kHz which is approximately the null-to-null bandwidth. Figure 8 is a plot of the Power Spectral Density (PSD) of a collected signal before the digital filter is applied and Figure 9 is a plot of the PSD of a collected signal after the digital filter is applied.

3.4.2 Burst Detection and Extraction.

This section details how each of the approximately 1000 bursts were extracted from each device. Following signal collection, the differential voltage signal for each steering angle sensor, S_{SAS} was formed by subtracting the CAN-Lo signal from the CAN-Hi signal. Next, an ideal reference signal, $refSig$, was generated, as shown in Figure 10, that corresponded to the symbol rate and bits in the preamble which includes Start of Frame, the Arbitration Field, and the Data Length Code and has a total of $N_{samp} = 40{,}000$ samples. Then, $refSig$ was cross correlated with each collected SAS signal, S_{SAS}, defined as

$$R_{XY}[m] = \sum_{n=1}^{L_{S_{SAS}}} refSig[n] \times S_{SAS_i}[n+m] \tag{15}$$

where $L_{S_{SAS}}$ is the length of each signal vector. The MATLAB® function $findpeaks$ was used to find the value that corresponded to the maximum correlation between $refSig$ and S_{SAS}. Each maximum value corresponded to the last index of the preamble ROI. Because the Data Field could also produce the same bit sequence as the

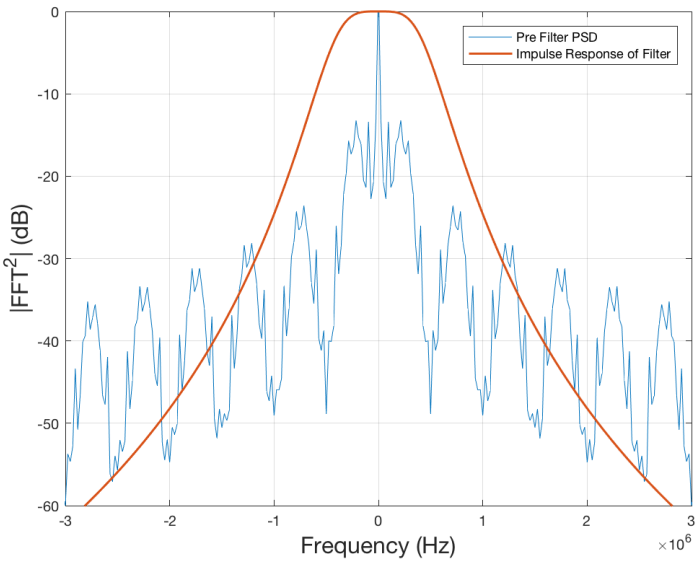

Figure 8. Power Spectral Density (PSD) of the Steering Angle Sensor (SAS) before applying digital filter.

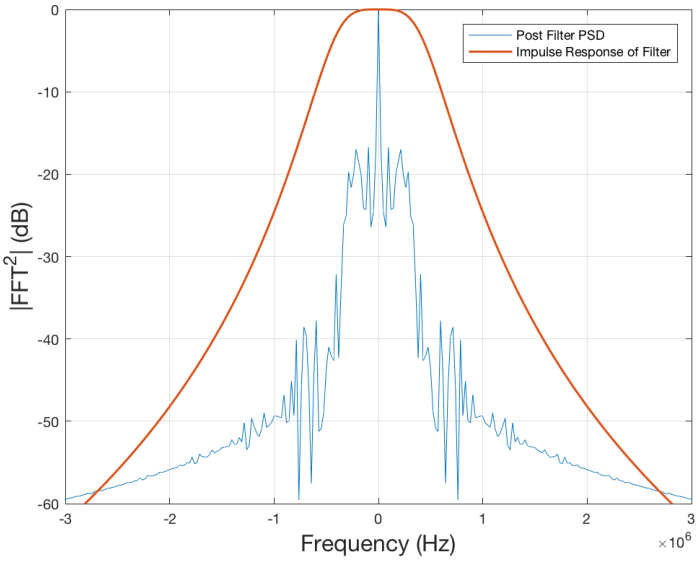

Figure 9. Power Spectral Density (PSD) of the SAS after applying digital filter.

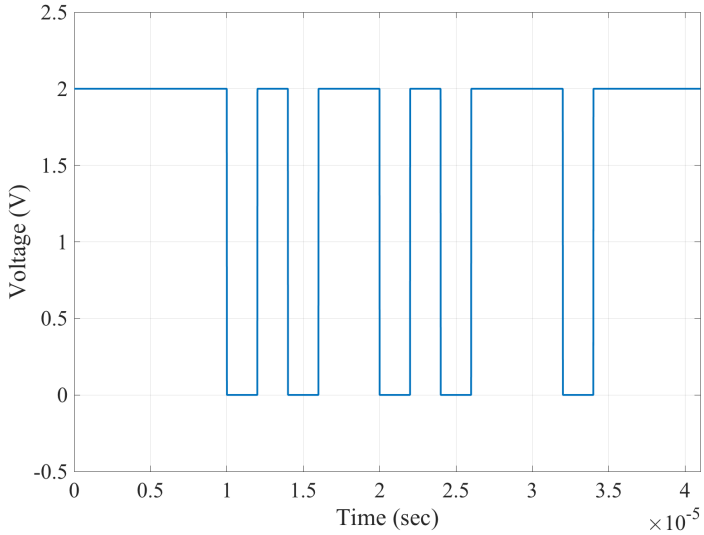

Figure 10. Ideal reference signal used for correlation based burst detection. The reference signal corresponds to the preamble of the Steering Angle Sensor (SAS).

$refSig$, $findpeaks$ only extracted data every $N_{samp} = 128{,}000$ samples. This number of samples represents the spacing between the end of the Data Length Code and the end of the Data Field. After each burst was extracted, it was placed in a matrix and aligned so that the first index of each burst is the first index of the noise region prior to the Start of Frame.

3.4.3 SNR Scaling.

This section provides an explanation of the necessity of generating multiple noise realizations for fingerprint generation. Although every effort was taken to reduce the effects of environmental noise, additive white Gaussian noise (AWGN) is assumed to be present from the power supply, the oscilloscope, and the collection probes. However, this noise does not demonstrate the effects of different channel conditions so different iterations of like-filtered, power-scaled independent AWGN were added during post-processing to simulate different channel conditions. For this experiment, noise was added that produced -46 $< SNR_{\Delta} <$ 0 decibels (dB) in 2 dB increments,

where SNR_{Δ} represents the reduction in SNR from collected conditions as the power of the AWGN is increased. For the purposes of this paper, SNR_{col} (collected conditions) denotes the SNR where classification performance is statistically equal to classification performance at SNR_C. For the 4-class and 9-class assessments, SNR_{col} is the same and is equal to $SNR_{\Delta} = 0$ dB. Additionally, $N_{MC} = 5$ independent Monte Carlo noise realizations were generated for each SNR_{Δ}. To be clear, SNR was never improved. Rather, AWGN was added to each burst until the average correct classification %C $\approx 1/N_C$.

3.4.4 Region of Interest (ROI).

This section presents the methodology used to identify the ROI which is a section of the signal that must be consistent and invariant in every burst. Within the SAS signal, the only fields that are constant in each frame are the Start of Frame, the Identification Field, the Data Length Code, the End of Frame, and the Interframe Spacing. Because of the potential for multiple ECUs to transmit simultaneously in

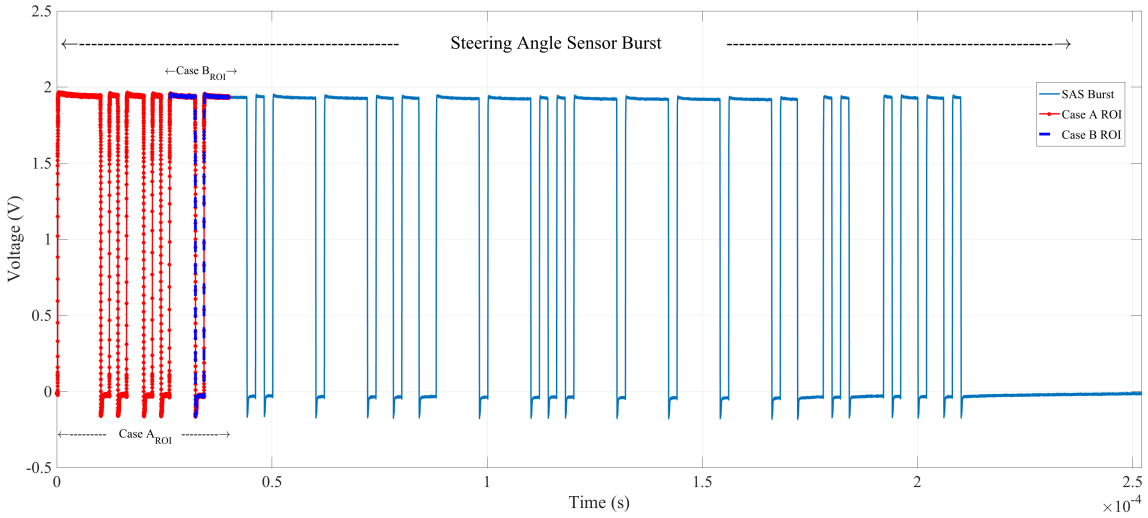

Figure 11. Typical SAS burst with the Region of Interest (ROI) highlighted for Case A and B.

the arbitration field, a second ROI was identified for implementation in a realistic base frame format CAN environment. The ROI that was selected for Case A included the Start of Frame, the Identification Field, and the Data Length Code. Case B only included the Remote Transmission Request bit, the ID Extension bit, the Reserved Bit, and the four Data Length Code bits. Figure 11 illustrates a typical collected base frame format message, or burst, as well as the selected ROI for Case A and Case B.

3.4.5 Signal-to-Noise Ratio Estimation.

The average collected Signal-to-Noise Ratio (SNR), SNR_C, was estimated by taking the ratio of the average power of the ROI (S_{Pow}) and the average power of the noise-like region in the End of Frame and Interframe spacing bits (N_{Pow}) resulting in $SNR_C \approx 43$ dB and calculated by

$$SNR_C = 10 \times \log_{10} \frac{(S_{Pow} - N_{Pow})}{N_{Pow}}. \tag{16}$$

The noise was assumed to be Gaussian and the calculation of S_{Pow} and N_{Pow} only considered the AC power[1]. The power calculations are displayed in decibels (dB) and the results of the estimation are shown in Table 3 and Table 4.

3.5 WS-DNA Fingerprinting

The composite fingerprints F_C^{WS} were generated for each Time Domain (TD) ROI by generating fingerprints in accordance with Section 2.5.1. Fingerprints were generated for the ideal, collision free environment to 1) assess the WS-DNA classification and verification performance using an entire invariant ROI and 2) use a comparable amount of bits to [8] to provide a performance estimate for WS-DNA implementa-

[1]For WS-DNA implementation, NRZ differential voltage signals should have power calculated using the variance as a power estimate.

tion on extended frame format ECUs. This set of fingerprints does not represent a realistic scenario on the CAN bus for base frame format ECUs because message collisions occur frequently but these fingerprints could be used to establish a baseline for ECUs prior to installation on a vehicle. A second set of fingerprints was generated to address the best ROI for WS-DNA implementation using base frame format ECUs on the CAN bus in a realistic environment.

3.5.1 Case A - Ideal Collision Free Environment.

Time Domain (TD) WS-DNA fingerprints are generated using the SAS preamble, which is composed of the Start of Frame, the Arbitration Field, and the Control Field, as the ROI. Additionally, $N_{samp} = 210$ samples were included before the SOF bit resulting in the ROI being composed of $N_{samp} = 40{,}000$ samples. The ROI was further divided into $N_R = 54$ contiguous subregions each containing $N_{samp} \approx 740$ samples. Subregion selection was determined empirically by fixing all fingerprint generation parameters while varying the number of subregions, N_R, and comparing the %C results. The N_R that produced the highest %C was chosen. For results that were

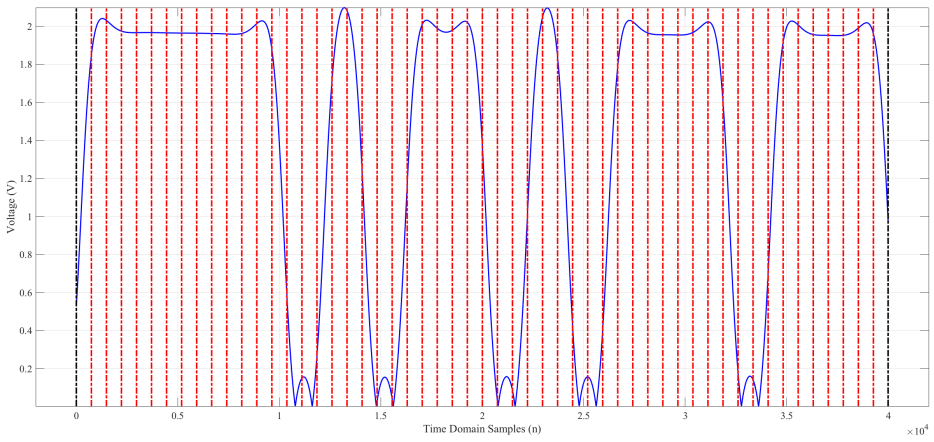

Figure 12. Steering Angle Sensor (SAS) Region of Interest (ROI) for Case A divided into 54 contiguous subregions.

statistically equal or indeterminate, the lower N_R was used to reduce the total number of features. The total number of features included in the WS-DNA fingerprints are composed of the $N_{resp} \times N_{stats} \times N_R + 1$, therefore, $N_{feats} = 3 \times 4 \times 55 = 660$ features. Fingerprints for the $N_{rg} = 3$ rogue devices were generated along with the authorized devices using the same fingerprint generation method. Figure 12 displays the ROI with the subregions denoted by the red dashed lines.

3.5.2 Case B - Realistic CAN bus environment.

TD WS-DNA fingerprints were generated to address a typical collision environment for base frame format ECUs excluding the Start of Frame and Arbitration Field that were included in Case A. The ROI for this scenario included the Remote Transmission Request bit, the ID Extension bit, the Reserved Bit, and the four Data Length Code bits. The ROI was divided in $N_R = 45$ subregions each containing $N_{samp} \approx 306$ samples. The total number of features included in the WS-DNA fingerprints are composed of the $N_{resp} \times N_{stats} \times N_R + 1$, therefore, $N_{feats} = 3 \times 4 \times 46 = 552$ features. Figure 13 displays the ROI with the subregions

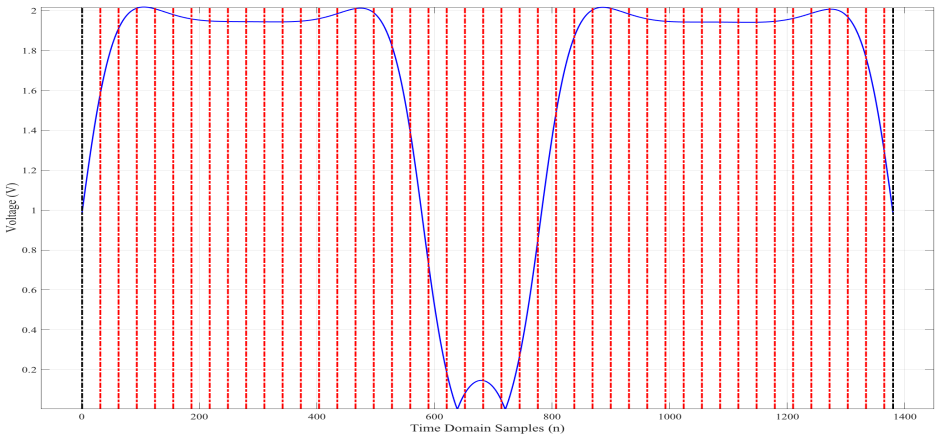

Figure 13. Steering Angle Sensor (SAS) Region of Interest (ROI) for Case B divided into 45 contiguous subregions.

denoted by the red dashed lines.

3.5.3 Rogue Devices.

To assess verification performance of the WS-DNA fingerprints, $N_{rg} = 3$ rogue devices were created to transmit the same bit level preamble as the authorized SAS devices. An Arduino Uno with a CAN shield, a Beagle Board with an ISO 1050 Can Transceiver, and a CANable CAN to USB adapter were used to create the rogue devices. The same, or similar, devices were used in previous research to simulate ECUs [2, 8]. The average differential voltage of the average SAS is compared to the average differential voltage of the three rogue devices in Figure 14. On average, the Beagle Board rogue device had a differential voltage that was 0.2 volts higher than the SAS and the other rogue devices.

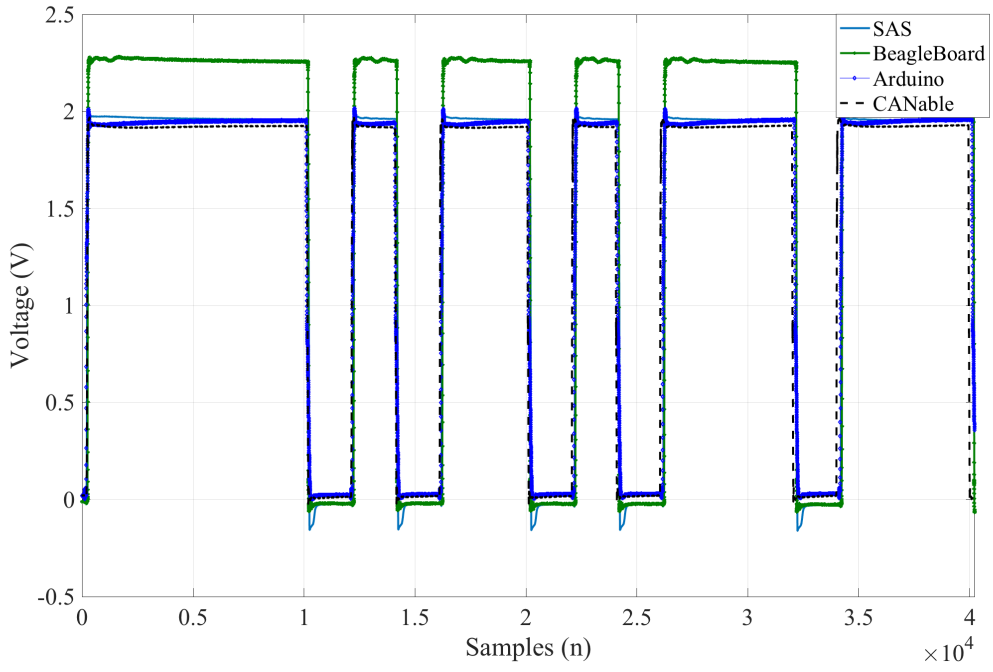

Figure 14. Average ROI differential voltage of all devices

3.6 Multiple Discriminant Analysis Maximum Likelihood (MDA/ML)

This section provides the methodology for classification and verification of the fingerprints that were generated in Section 3.5.

3.6.1 Classification.

$N_{bursts} \approx 1000$ WS-DNA fingerprints for all $N_C = 4$ and $N_C = 9$ classes were used for classification. A total of $N_{NZ} = 5$ noise realizations were generated resulting in a total of $N_{bursts} \approx 5000$ bursts that were available for MDA/ML implementation. $N_{prints} \approx 2500$ were used for MDA/ML model development and $N_{prints} \approx 2500$ were used for testing. For both the training and testing fingerprints, approximately 2500 interleaved fingerprints from each class were used because collections were taken at different times and temperatures, and are therefore subject to varying environmental and collection bias. Following the training phase, the model was validated using K-Fold Cross Validation. Based on previous work, a value of K=5 was used for K-Fold Cross Validation [3, 24, 28, 33, 36, 40]. As described previously in Section 2.5, K-Fold validation partitions the fingerprints into K equal sections and trains on K-1 sections, after which the partition that was held out is tested. This process was repeated K times and the best performing model is chosen for the classifier. MDA/ML classification results are presented graphically as the average percent correct classification (%C) for each SNR. Figure 15 displays the average correct classification for a $N_C = 4$ class problem as SNR is increased via a decrease in the power of the added AWGN.

3.6.2 Verification.

This section provides an overview of the methodology used to achieve device verification. The purpose of device verification is to measure device similarity and assess

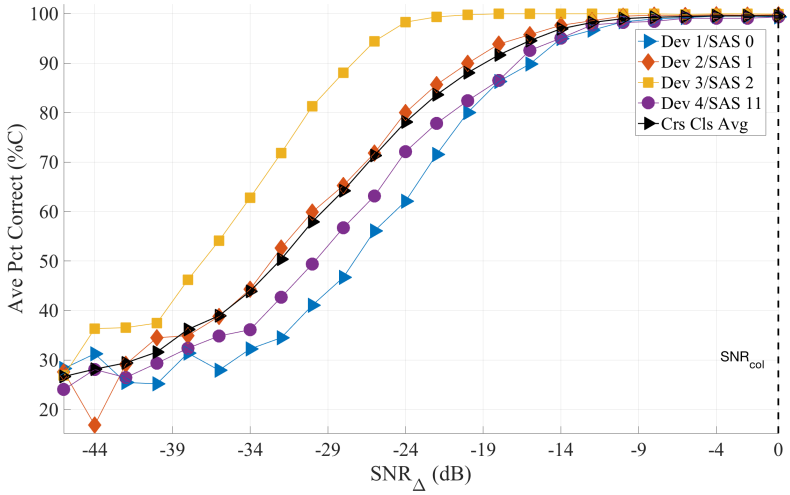

Figure 15. MDA/ML classification testing results for $N_C = 4$ class Cross Lot Discrimination (CLD) assessment.

the rate at which a rogue device is accepted or rejected. To measure device similitude, a test statistic Z_V is generated based on common features from the testing and training fingerprints. A probability mass function (PMF) was generated from Z_V of each authorized device and a threshold was established that corresponded with a True Verification Rate (TVR) $> 90\%$ and a False Verification Rate (FVR) $< 10\%$. An unknown devices' fingerprints were presented and the same process for generating a test statistic was applied to these fingerprints. These fingerprints were classified (rightly or wrongly) based on which side of the threshold they fell on. Verification was assessed using Euclidean Distance as a measure of similarity and Equal Error Rate (EER) $= 10\%$ as a measure of success. EER is the device dependent metric chosen for this experiment where the TVR is equal to the Rogue Rejection Rate (RRR). TVR is calculated as the number of attempts by an authorized device that are correctly accepted divided by the total number of attempts and RRR is calculated as the total number of rogue attempts that are correctly rejected divided by the total number of rogue attempts. Results from the Device Verification process are presented graphically on a Receiver Operating Characteristic (ROC) curve as a comparison of the

TVR versus the FVR and TVR versus RAR where RAR is equal to one minus RRR. Figure 16 displays results of the MDA/ML verification process for a $N_C = 4$ class CLD problem. An alternate presentation for the ROC curve is shown in Figure 17. This stem plot is a burst-by-burst (BbB) assessment used to display the authorized device verification results [3]. The horizontal black lines denote the device dependent EER threshold, the red X's denote access incorrectly denied, and the blue circles denote access correctly granted.

Rogue device acceptance was measured by using the rogue devices as well as by using all authorized devices as rogue, or compromised, devices and assessing how often these devices were accepted when falsely presenting an authorized device's credentials. These results are also presented graphically as a measure of TVR versus Rogue Acceptance Rate (RAR). Figure 18 displays an alternate way to present the rogue assessment results; a burst-by-burst grant/deny access decision. The horizontal black lines on the plot represent the device dependent EER thresholds that were generated for each class, the blue circles represent the fingerprints that were correctly rejected, and the red X's represent the fingerprints that were incorrectly accepted. In the N_C

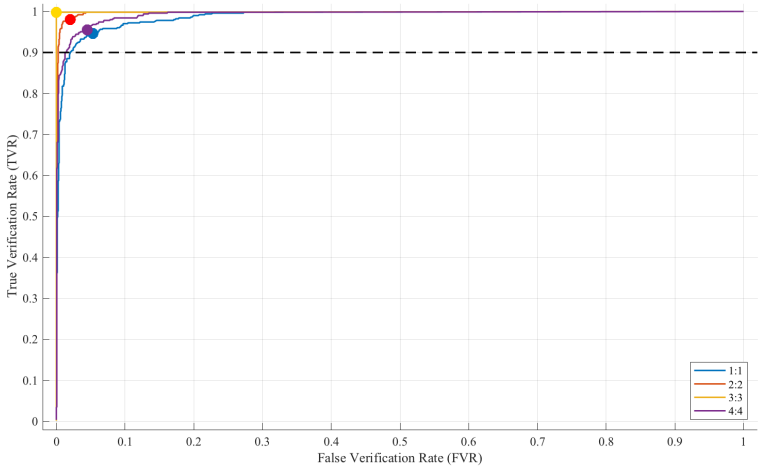

Figure 16. An example of results of MDA/ML verification for $N_C = 4$ class assessment.

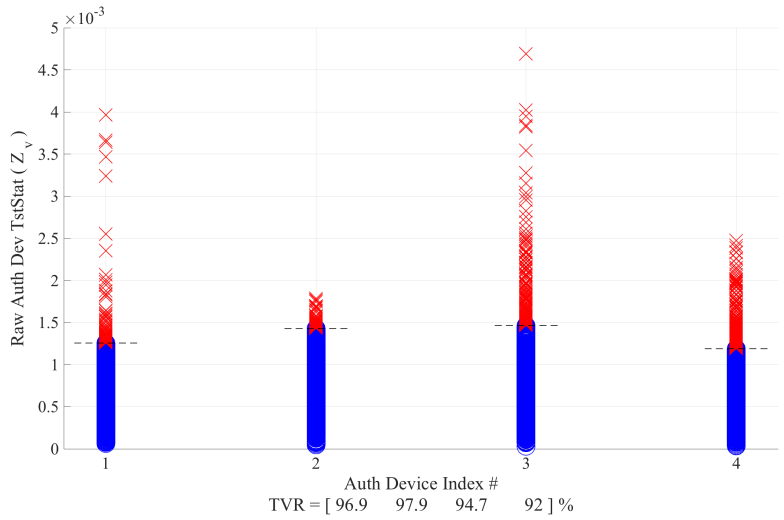

Figure 17. An example of True Verification results for a $N_C = 4$ class problem. Results are an alternate presentation of the ROC curve and are presented as a burst-by-burst grant/deny access assessment.

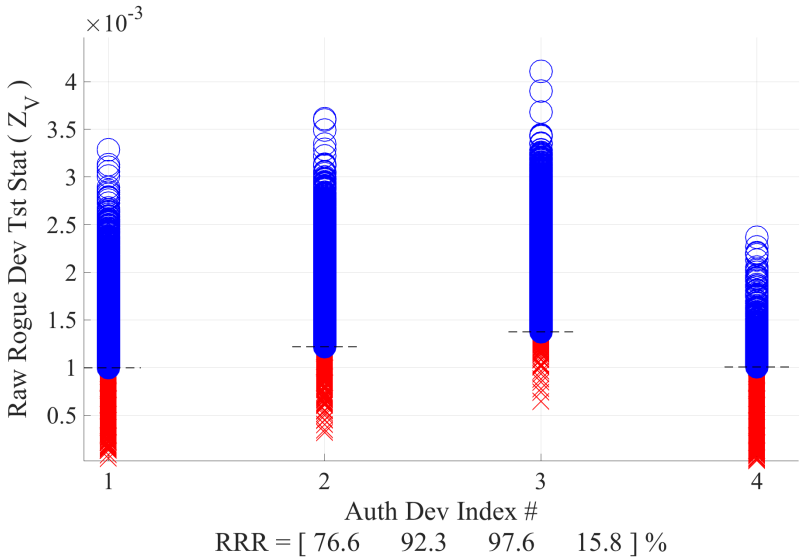

Figure 18. An example of results from the rogue assessment for a $N_C = 4$ class problem where Device 4 falsely presents credentials for each authorized device. Results are an alternate presentation of the ROC curve and are presented as a burst-by-burst grant/deny access assessment.

= 4 class problem presented in the plot, Device 4 falsely presents credentials for each authorized device.

IV. Results

This chapter begins with an analysis of the differences between the transition from a dominant bit to a recessive bit for the authorized devices compared to the rogue devices. This analysis is presented in Section 4.1 and is vital to the results discussion. The results of the Wired Signal Distinct Native Attribute (WS-DNA) device classification and device verification for $N_C = 4$ class Cross Lot Discrimination (CLD) and $N_C = 9$ class Like Model Discrimination (LMD) are presented in Section 4.2. Additionally, the results for $N_C = 6$ and $N_C = 3$ class thermal cycling problems are presented. Lastly, $N_C = 3$ class CAN transceiver classification results are presented as a first-look assessment of thermal effects on device classification. WS-DNA fingerprinting was implemented in accordance with the methodology described in Section 3.6. Classification results are displayed as average percent correct classification (%C) for the 1 vs M assessment to determine which device the fingerprints looks most like and presented in Section 4.2. Device verification is presented as Rogue Rejection Rate (RRR), Rogue Acceptance Rate (RAR), True Verification Rate (TVR), and False Verification Rate (FVR) for the 1 vs 1 "looks how much like" assessment and is presented in Section 4.3. The $N_C = 4$ class and $N_C = 9$ class discrimination results are presented for the two different ROI's generated in accordance with Section 3.5. All results are presented at SNR_{col} where %C is statistically equal to performance at the average collected SNR (SNR_C)[1]. The same range of SNR_Δ is used for classification plots for the 4-class and 9-class assessments to provide a comparison of CLD and LMD at the same SNRs. Thermal cycling results are presented in Section 4.4 using $N_C = 6$ and $N_C = 3$ class thermal assessments. Additionally, $N_C = 3$ class, Cross Lot, Cross Temperature classification results are presented in this section.

[1] SNR_{col} is approximately 20 dB less that SNR_C but all results for $SNR_{col} \leq \%C \leq SNR_C$ are statistically equal and were omitted from the classification plots.

4.1 ECU Transition Misalignment

This section is presented to discuss the symbol rate and transitions of the authorized Electronic Control Units (ECU) compared to the $N_{rg} = 3$ rogue devices that have been used to emulate ECUs [2, 7]. Figure 19 displays an expanded view of the first transition from a dominant bit to a recessive bit for the average Steering Angle Sensor (SAS) as well as the Arduino, Beagle Board, and CANable. It is clear that the SAS reaches a much lower voltage than the rogue devices as it transitions which provides critical information for discrimination. Also, each of the rogue devices are not perfectly aligned with the SAS and all rogue devices have a unique ripple effect as they transition to the recessive bit. The devices continue to transmit at a slightly different symbol rate for the remainder of the data frame resulting in further misalignment at the end of the Region of Interest (ROI), which can be seen in Figure 19. These features are likely the reason why rejection rates are high for LMD and CLD assessment which will be explained in Section 4.3.

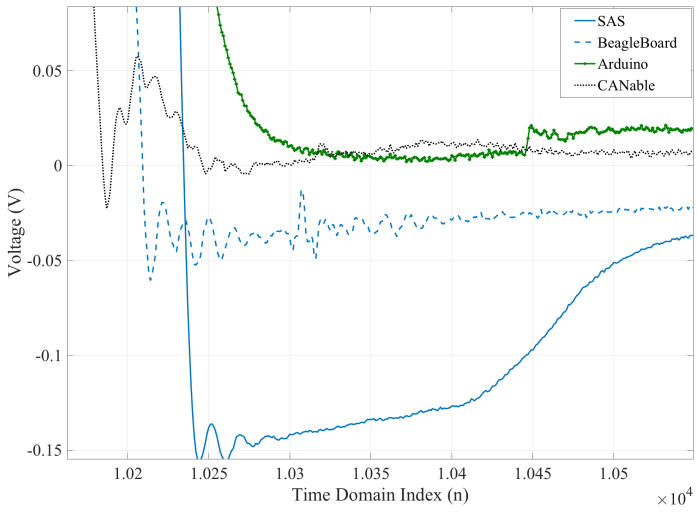

Figure 19. Expanded view of the average bit transition from dominant to recessive for the SAS and $N_{rg} = 3$ rogue devices.

4.2 Device Classification

This section includes the results for the device classification of Toyota Steering Angle Sensors using WS-DNA and MDA/ML as outlined in Section 3.5. Classification results are displayed graphically and with confusion matrices for $N_C = 4$, Cross Lot Discrimination, and $N_C = 9$, Like Model Discrimination. A total of $N_{bursts} \approx 1000$ bursts with $N_{trng} = N_{test} \approx 500$ interleaved fingerprints were used for training and testing for each device. Furthermore, five like-filtered Additive White Gaussian Noise (AWGN) realizations were generated for each fingerprint per device. This resulted in $N_{trng} \approx 500 \times 5 \approx 2500$ fingerprints and $N_{test} \approx 500 \times 5 \approx 2500$ fingerprints per device for the Cross Lot Discrimination assessment and Like Model Discrimination assessment. The AFIT RF-DNA arbitrary benchmark of %C = 90% was used for the average correct classification measure of success and all results are based on 95% confidence intervals. For all classification plots, the confidence intervals fall within the vertical extent of the markers and were omitted for visual clarity.

4.2.1 4 Class Cross Lot Discrimination.

The first experiment was the $N_C = 4$ class CLD problem of steering angle sensors of the same part number each with a different lot number. The classification results are presented in Figure 20 where %C = 90% is achieved at $SNR_\Delta \geq$ -19 dB for Case A with the maximum %C $\geq$ 99% achieved at $SNR_\Delta \geq$ -10 dB. Device 3 has a statistically significant increase in correct classification over all other devices from $SNR_\Delta \geq$ -39 dB to $SNR_\Delta =$ -14 dB. Upon inspection, Device 3 was verified to have the newest internal components. The classification results for Device 2 are statistically equal to the cross class average. A comparison of the the cross class average %C for Case A (entire preamble) and Case B (No Arbitration Field) is shown in Figure 21. Case A classification results are statistically better than results from Case B at SNR_Δ

$\geq$ -40 dB. For Case B, %C $\geq$ 90% is achieved at $SNR_{\Delta} \approx$ -10 dB.

Confusion matrix results are presented in Table 6 as %C Case A (Bold text)/ %C Case B. There is degraded classification performance when the Arbitration Field is excluded from the ROI. Classification performance for Device 1 and 4 is reduced by approximately 5% and classification performance for Device 2 and 3 is reduced by approximately 2%. Device 1 and 4 were confused the with each other more than with the other devices. It should be noted that these devices were both obtained from

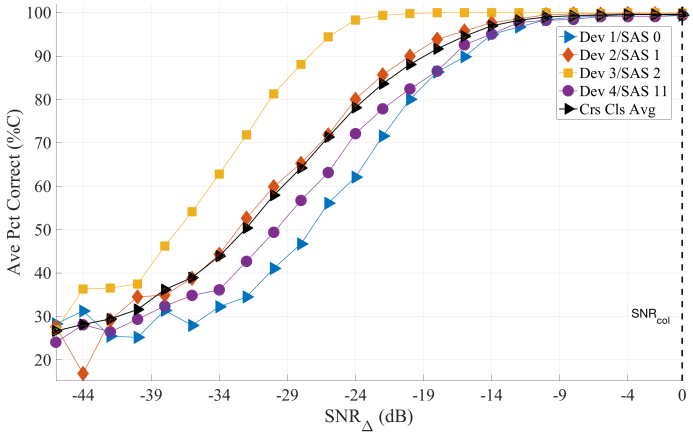

Figure 20. Results from MDA/ML 4 Class Cross Lot Classification for Case A. %C = 90% is achieved at $SNR_{\Delta} \geq$ -14 dB

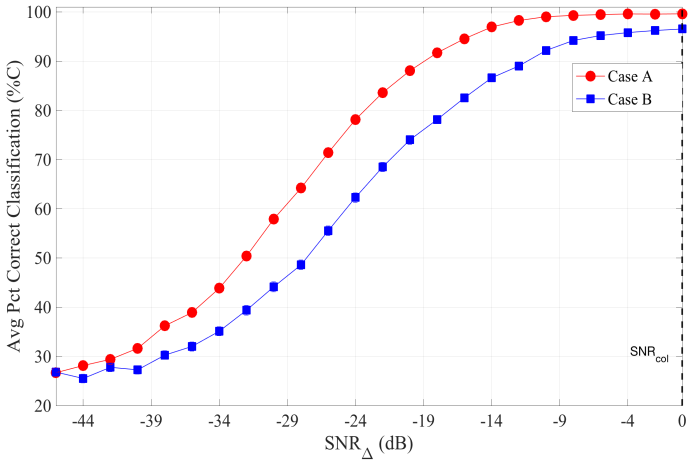

Figure 21. MDA/ML Classification Results for Cross Class Average using Case A and Case B ROI for N_C = 4 class CLD

Table 6. Cross Lot Discrimination Confusion Matrix (%) for $N_C = 4$ classes at SNR_{col}. Results are displayed as %C Case A (entire preamble) / %C Case B (no Arbitration Field).

	Dev 1	Dev 2	Dev 3	Dev 4
Dev 1	**99.6**/93.76	**0**/1.88	**0**/0	**0.4**/4.36
Dev 2	**0.04**/1	**99.6**/97.8	**0**/0.04	**0**/1.16
Dev 3	**0**/0.56	**0.04**/1.04	**99.92**/97.88	**0.04**/0.52
Dev 4	**0.28**/2.76	**0.2**/1.92	**0**/0.12	**99.52**/95.2

used vehicles. As SNR was degraded, Device 1 and 4 were incorrectly classified as each other more than other devices which may indicate that these devices look more similar to each other as they age.

The results in this section indicate that $> 90\%$ correct identification of similar components is achievable using WS-DNA fingerprints generated from Case B. Correct classification (%C) $\geq 90\%$ for realistic implementation can still be achieved even when SNR is degraded by 10 dB.

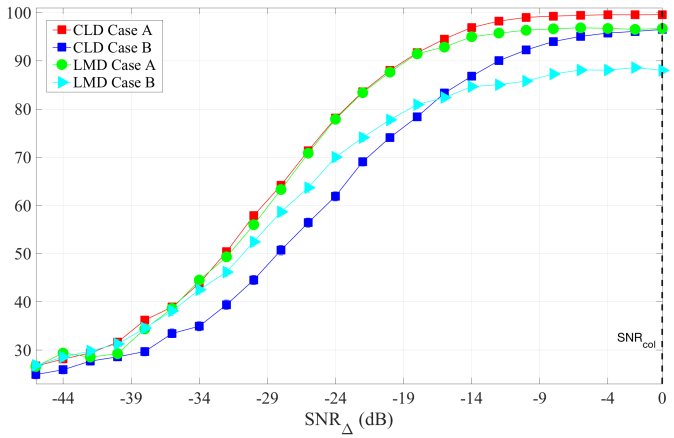

Figure 22. Comparison of Cross Class Average for Cross Lot Discrimination and Like Model Discrimination for Case A and Case B.

4.2.2 Comparison of $N_C = 4$ Class CLD and $N_C = 4$ Class LMD.

This section provides a direct comparison of the cross class average correct classification for the Cross Lot Discrimination and Like Model Discrimination. The CLD results are the same results presented in the previous section and the LMD results were generated using the arbitrarily chosen Device 1, 2, 6 and 7 from the $N_C = 9$ class assessment. Results for Case A and Case B are presented for both assessments and shown in Figure 22. CLD results for Case A are statistically better than the other assessments at $SNR_\Delta >$ -14 dB. LMD results for Case B are statistically worse than the other assessments at $SNR_\Delta >$ -14 dB and this assessment fails to meet the success criteria of %C $\geq$ 90%. These results indicate that the WS-DNA fingerprints generated would not be viable for implementation on the CAN bus if four or more base frame format devices of the same make and model are present.

4.2.3 9 Class Like Model Discrimination.

9 Class LMD device classification consisted of 9 sensors from lot 823F. The Case A classification results in Figure 23 are for -46 $\geq SNR_\Delta \geq$ 0 dB with the arbitrary %C = 90% achieved at $SNR_\Delta \geq$ -4 dB based on 95% confidence intervals. Device 2 and Device 7 had statistically better %C than the other seven classes for all SNR_Δ above -38 dB and were correctly classified at least 90% of the time at $SNR_\Delta \geq$ -20 dB. A direct comparison of classification performance for Case A versus Case B is presented in Figure 24. Case A has statistically better performance than Case B for $SNR_\Delta \geq$ -32 dB and %C = 90% was not achieved for Case B at any SNR_Δ including collected conditions.

The 9 class LMD confusion matrix results for Case A and Case B are presented in Table 7 and 8 respectively. Case A has an average %C at this SNR that is $\approx$ 20% better than Case B. Device 2 and Device 7 are the best performing devices achieving

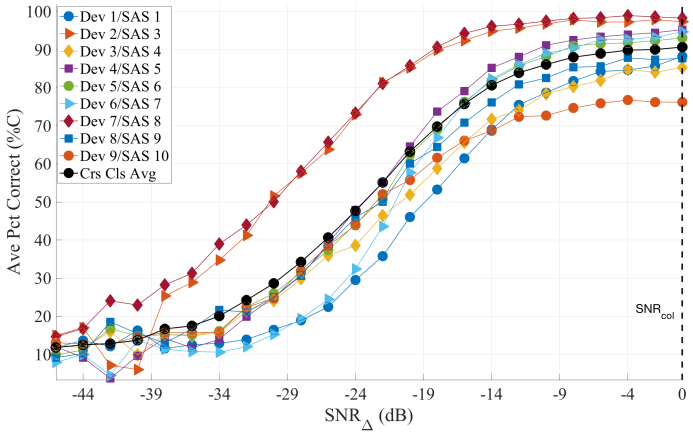

Figure 23. Results from MDA/ML 9 Class Like Model Classification for Case A. %C = 90% is achieved at $SNR_{\Delta} \geq$ -4 dB.

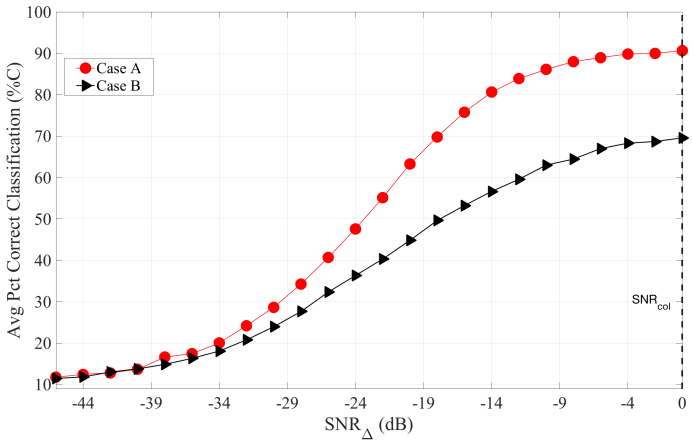

Figure 24. MDA/ML Classification Results for Cross Class Average using Case A and Case B ROI for N_C = 9 Class Like Model Classification.

%C $\geq$ 97% for Case A and %C $\geq$ 85% for Case B. Device 1, 3, 8, and 9 all fail to achieve %C $\geq$ 90% for Case A and all fail to achieve %C $\geq$ 65% for Case B. For both cases, Device 3 and Device 9 look most like each other and Device 2 and Device 7 look the least like any other device. The differences and similarities of all of these devices likely result from the subcomponents such as the CAN transceiver and the Control Unit, which are displayed in Table 2. All devices had the same markings on the transceiver but there were two different part, or lot, numbers present for the Control Unit. Device 2 and 7 were both part number 1736 E08 but Device 3 and

Table 7. Confusion matrix for $N_C = 9$ Class assessment at SNR_{col} for Case A

	Dev 1	Dev 2	Dev 3	Dev 4	Dev 5	Dev 6	Dev 7	Dev 8	Dev 9
Dev 1	86.52	5.4	0	0	3.08	0.12	0	4.88	0
Dev 2	2.12	97.72	0	0.16	0	0	0	0	0
Dev 3	0	0	84.64	0	0	1.04	1.32	0	13
Dev 4	0.2	0.24	0.24	95.28	0	4.04	0	0	0
Dev 5	1.76	0	0	0	92.84	0.04	0	5.36	0
Dev 6	0.88	0	1.28	2.68	0.16	94.08	0	0.12	0.8
Dev 7	0	0	0.88	0	0	0	98.28	0	0.84
Dev 8	5.44	0.08	0	0	6.84	0	0	87.64	0
Dev 9	0	0	20.24	0	0	1.12	1.16	0	77.48

Table 8. Confusion matrix for $N_C = 9$ Class assessment at SNR_{col} for Case B

	Dev 1	Dev 2	Dev 3	Dev 4	Dev 5	Dev 6	Dev 7	Dev 8	Dev 9
Dev 1	57.6	10.44	0.12	4.84	6.96	3.4	0	16.56	0.08
Dev 2	9.12	85.48	0	5.12	0	0	0	0.28	0
Dev 3	0	0	60.32	1.76	0.16	8.2	10.48	0	19.08
Dev 4	4.16	4.6	1.52	74.64	0.04	14.36	0	0.16	0.52
Dev 5	6.48	0.04	0.04	0.12	75.4	3.4	0	14.44	0.08
Dev 6	5.56	0	6.08	9.44	2.28	65.64	0.76	1.84	8.4
Dev 7	0	0	6.88	0	0	0.2	85.52	0	7.4
Dev 8	15.2	1.56	0	0.4	17.4	2.08	0	63.36	0
Dev 9	0	0	21.24	0.32	0.08	11.8	8.96	0	57.6

9 were different part numbers, indicating that another subcomponent, such as the transceiver, may have been responsible for the confusion.

The $N_C = 9$ class classification results indicate that WS-DNA implementation using Case A is viable for correctly classifying Like Model devices on the CAN bus $> 90\%$ of the time. If devices do start transmitting more similar signals as they age, WS-DNA would likely not be effective for properly classifying $N_C \geq 9$ devices of the same make and model on the CAN bus.

4.3 Device Verification

Device verification is a one versus one measure of similarity and was assessed here for authorized and rogue devices for Cross Lot Discrimination and Like Model

Discrimination. $N_{rg} = 3$ rogue devices that were used included an Arduino, a BeagleBone, and a CANable all transmitting the same arbitration ID of a Toyota Steering Angle Senor as well as each authorized device simulating a compromised device. Device verification was achieved using Euclidean distance test statistic as a measure of similarity and Equal Error Rate (EER) = 10 % as a measure of success. Devices are either granted or denied access based on whether the test statistic (Z_V) is greater than or less than the device dependent threshold ($t_V(d)$). Verification results are presented at SNR_{col}.

4.3.1 4 Class Cross Lot Discrimination.

The results for the Authorized Device ID verification are displayed in Figure 25 and 26. Grant/deny access decisions were assessed using $N_{prints} \approx 2500$ fingerprints. The horizontal black dashed line represents the arbitrary threshold of True Verification Rate (TVR) $\geq$ .9 which is consistent with previous RF-DNA work [3, 9, 33, 36, 40]. For both cases, the solid ROC curves indicate that all four devices met the arbitrary benchmark of TVR $\geq$ .9 and FVR $\leq$ .1 at SNR_{col}. The burst-by-burst TVR assessment results are presented in Figure 27 and 28 and included for completeness. The horizontal black lines denote the device dependent threshold set for a training threshold of TVR = 90%, the red X's indicate access incorrectly denied, and the blue O's denote access correctly granted. TVR results at SNR_{col} for Case A are approximately 95% and results for Case B are approximately 91% for the four devices.

The results for the Rogue Device ID verification are presented in Figure 29 and 30. Rogue ID verification is the process where rogue devices present false credentials and are either accepted or rejected as the device they are claiming based on the threshold ($t_V(d)$) established from the PMF. The dashed black box represents the area where the TVR $\geq$ .9 and the RAR $\leq$ .1. The black stars on each line represent the device

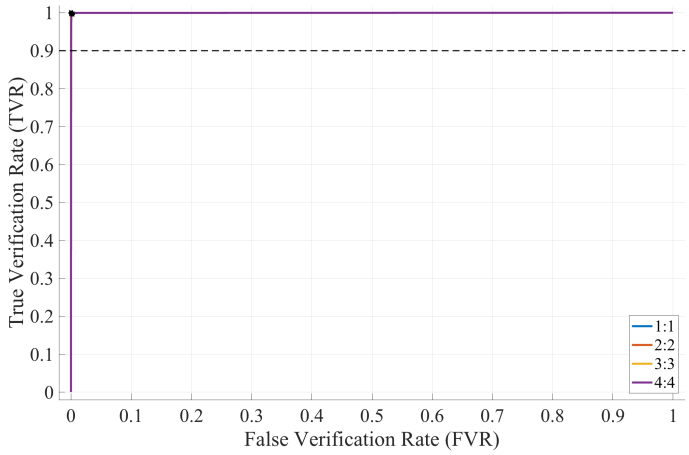

Figure 25. Device ID Verification ROC curve for $N_C = 4$ Class Cross Lot Discrimination (CLD) at SNR_{col} for Case A using Euclidean distance as a measure of similarity. All devices achieved True Verification Rate (TVR) $\geq$ .9 and False Verification Rate $\leq$ .1.

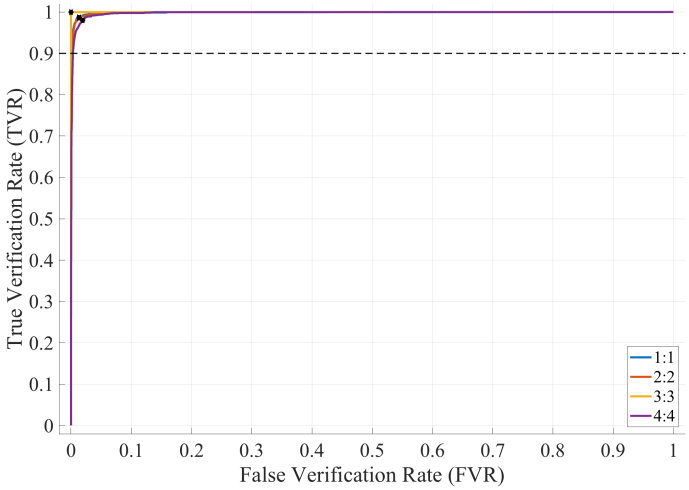

Figure 26. Device ID Verification ROC curve for $N_C = 4$ Class Cross Lot Discrimination (CLD) at SNR_{col} for Case B using Euclidean distance as a measure of similarity. All devices achieved True Verification Rate (TVR) $\geq$ .9 and False Verification Rate $\leq$ .1.

dependent EER and the solid curves denote successful verification. For both cases, all devices successfully met the EER success criteria.

Figure 31 and 32 provide an alternate presentation of the Rogue Device ID verification. These results are only for rogue devices claiming Device 1's ID, but results were consistent for all authorized devices. These verification results are based on a burst-by-burst grant/deny access criteria [6]. The O's represent access correctly

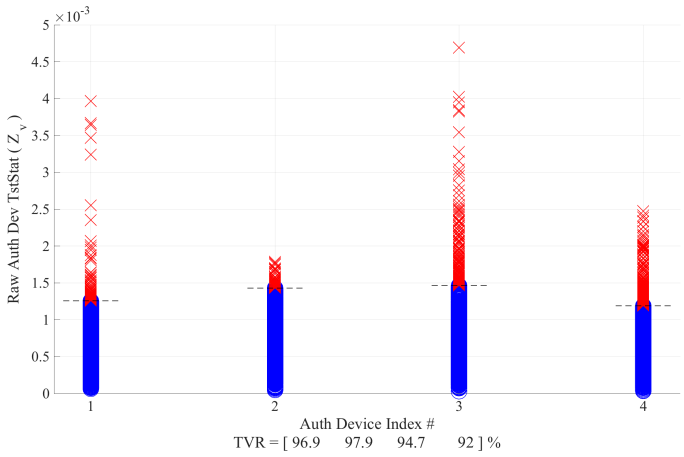

Figure 27. Device ID Verification stem plots for $N_C = 4$ Class Cross Lot Discrimination (CLD) at SNR_{col} for Case A using Euclidean distance as a measure of similarity. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx$ 2500 authorized attempts. Red X's indicate access incorrectly denied and blue circles indicate access correctly granted. The average TVR was approximately 95%.

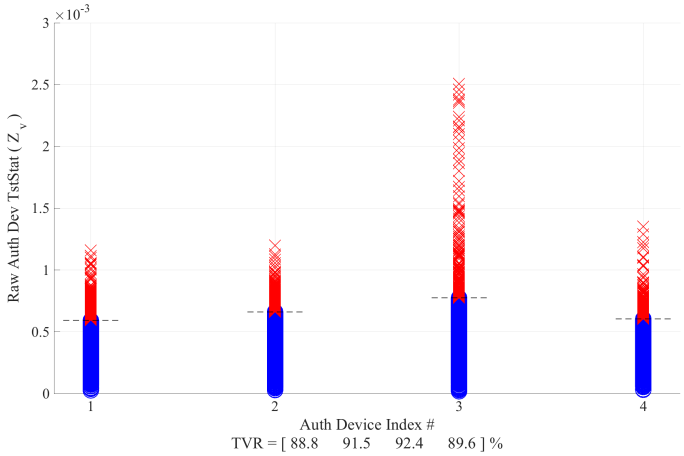

Figure 28. Device ID Verification stem plots for $N_C = 4$ Class Cross Lot Discrimination (CLD) at SNR_{col} for Case B using Euclidean distance as a measure of similarity. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx$ 2500 authorized attempts. Red X's indicate access incorrectly denied and blue circles indicate access correctly granted. The average TVR was approximately 91%.

denied and the X's indicate access incorrectly granted. The horizontal black lines are the device dependent EER thresholds which are ≈ 0 on the plots. For Case A, all rogue devices were denied access for 100% of their attempts as each authorized device. The RRR results are also 100% for Case B and are presented in Figure 32. Rogue Device 3 looks less like Device 1 for Case B which is likely attributable to

the symbol and transition misalignment which can be observed in Figure 19. The verification results for Device 4 presenting false credentials for all authorized devices are shown in Figure 33 and Figure 34. Excluding the results for Device 4 presenting its own credentials, the average RRR is $\approx 100\%$ when a compromised ECU attempts to present false credentials for Case A. For Case B, the average RRR was approximately 99%. Overall, Rogue Rejection Rates are high for the unauthorized devices

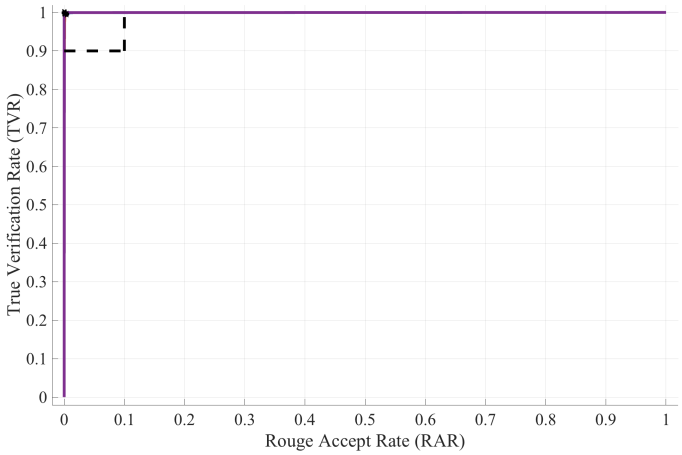

Figure 29. Rogue Device ID Verification ROC curve for $N_C = 4$ Class CLD at SNR_{col} for Case A using Device 4 and $N_{Rg} = 3$ rogue devices. All devices achieved TVR $\geq$ .9 and RAR $\leq$ .1.

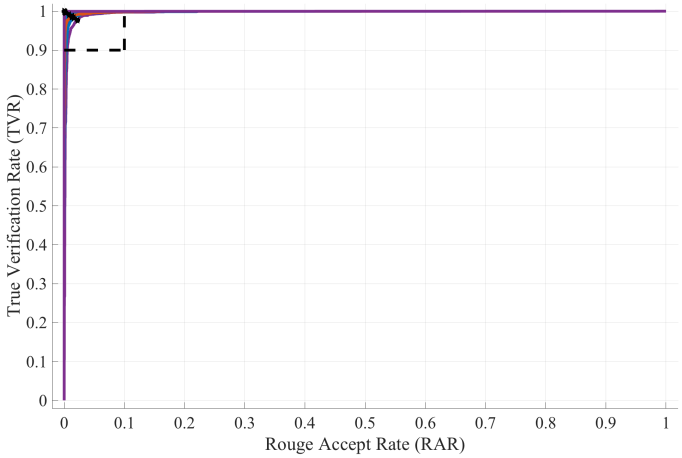

Figure 30. Rogue Device ID Verification ROC curve for $N_C = 4$ Class CLD at SNR_{col} for Case B using Device 4 and $N_{Rg} = 3$ rogue devices. All devices achieved TVR $\geq$ .9 and RAR $\leq$ .1.

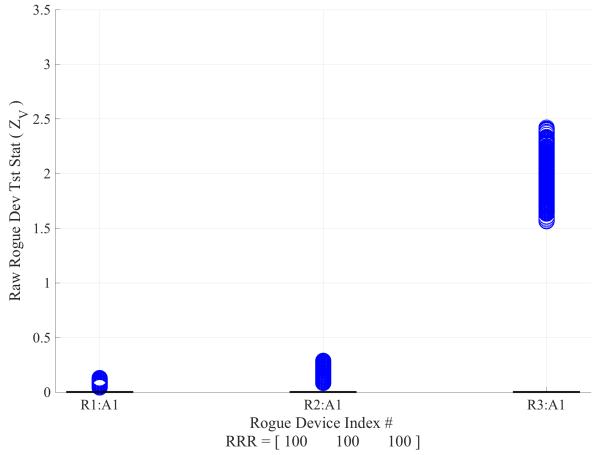

Figure 31. Rogue Device Verification at SNR_{col} for Case A using $N_{Rg} = 3$ rogue devices. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx 5000$ rogue attempts. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied. All rogue devices were rejected 100% of the time when falsely presenting Device 1's credentials.

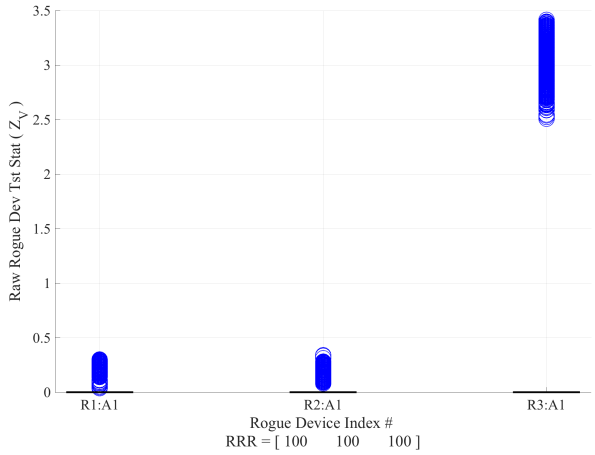

Figure 32. Rogue Device Verification at SNR_{col} for Case B using $N_{Rg} = 3$ rogue devices. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx 5000$ rogue attempts. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied. All rogue devices were rejected 100% of the time when falsely presenting Device 1's credentials.

likely because each device is unable to accurately match the symbol rate resulting in drastic differences in the transition regions at the nanosecond level as shown in Figure 19. Although Rogue Device 1 has a higher average amplitude than the other devices, the bit transitions are more aligned with the SAS than Rogue Device 3 resulting in a higher degree of similarity. Based on the results for the $N_C = 4$ Class

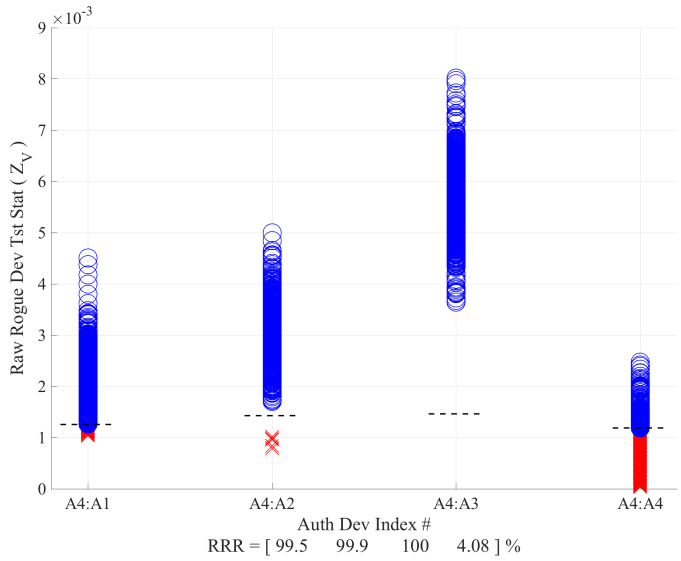

Figure 33. Rogue Device Verification at SNR_{col} for Case A using Device 4 as the rogue device. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied. Device 4 was rejected $\approx$ 100% of the time when falsely presenting credentials for Device 1-3.

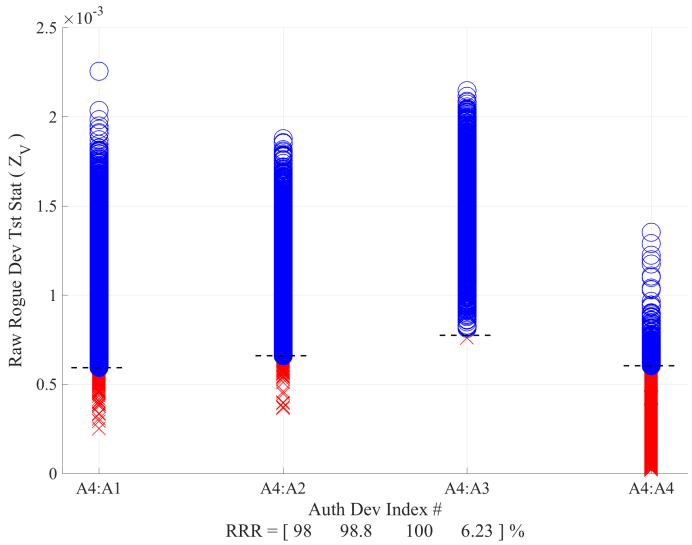

Figure 34. Rogue Device Verification at SNR_{col} for Case B using Device 4 as the rogue device. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied. Device 4 was rejected $\approx$ 99% of the time when falsely presenting credentials for Device 1-3.

CLD assessments shown in Table 9, WS-DNA is a viable method for establishing or augmenting security on the CAN bus. Unauthorized device attempts were rejected $>$ 90% of the time even when SNR was degraded by 39 dB and rejected 100% of the

time when SNR was degraded by 29 dB. Compromised device attempts were rejected $> 90\%$ of the time when SNR was degraded by 14 dB.

Table 9. Average Rogue Rejection Rates (%) for all 4 class rogue assessments at each SNR_{Δ}. 12 unauthorized and 9 compromised rogue rejection assessments were completed at each SNR_{Δ}.

	$\text{SNR}_{\Delta}(dB)$	-44	-39	-34	-29	-24	-19	-14	-9	-4	0
Case A	Compromised	55.39	64.03	63.42	73.01	85.24	93.34	98.05	99.50	99.81	99.88
	Unauthorized	91.33	99.78	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
Case B	Compromised	53.80	54.21	56.08	63.45	72.43	84.48	91.97	96.26	98.71	99.24
	Unauthorized	80.29	94.89	99.99	100.00	100.00	100.00	100.00	100.00	100.00	100.00

4.3.2 9 Class Like Model Discrimination.

This section provides the verification results for the $N_C = 9$ Class LMD assessment at SNR_{col} (collected conditions). Figures 35 and 36 display the Device ID verification ROC curves at SNR_{col}. The dashed lines denote devices that did not achieve the arbitrary benchmark of TVR $\geq .9$ and FVR $\leq .1$ and the solid lines denote successful verification performance. For Case A, all devices met the success criteria but for Case B, only Devices 2, 4, and 7 met the threshold. Device 2 and 7 were the most dissimilar devices during device classification and these verification results are consistent with the classification results. The burst-by-burst TVR assessment results are presented in Figure 37 and 38 and included for completeness. The horizontal black lines denote the device dependent threshold set for a training threshold of TVR $= 90\%$, the red X's indicate access incorrectly denied, and the blue O's denote access correctly granted. TVR results at SNR_{col} for Case A are approximately 87% and results for Case B are approximately 80% for the nine devices.

Figures 39 and 40 present the Rogue Device ID verification results when Device 9 and $N_3 = 3$ rogue devices falsely presented credentials for all authorized devices. The solid curves denote devices that achieved the arbitrary benchmark of TVR $\geq .9$ and RAR $\leq .1$ and the dashed curves denote devices that failed to meet the threshold.

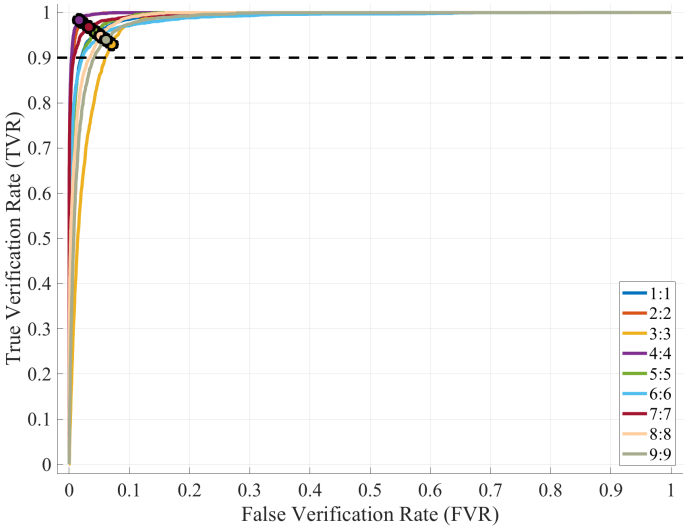

Figure 35. Device ID Verification ROC curve for $N_C = 9$ Class Like Model Discrimination (LMD) at SNR_{col} for Case A. Verification is achieved using Euclidean distance as a measure of similarity. 9/9 devices met the success criteria of TVR $\geq$ .9 and FVR $\leq$ .1.

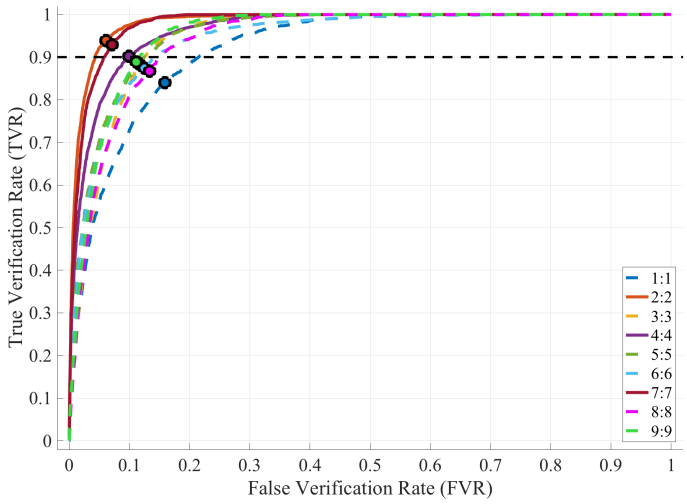

Figure 36. Device ID Verification ROC curve for $N_C = 9$ Class Like Model Discrimination (LMD) at SNR_{col} for Case B. Verification is achieved using Euclidean distance as a measure of similarity. Only 3/9 devices met the success criteria of TVR $\geq$ .9 and FVR $\leq$ .1.

Case A results are presented in Figure 39 and indicate that all devices were successful except Device 3 (dashed curve). Case B results are presented in Figure 40 and show that Device 3, 6, and 7 did not achieve TVR $\geq$ .9 and RAR $\leq$ .1 when Device 9 was

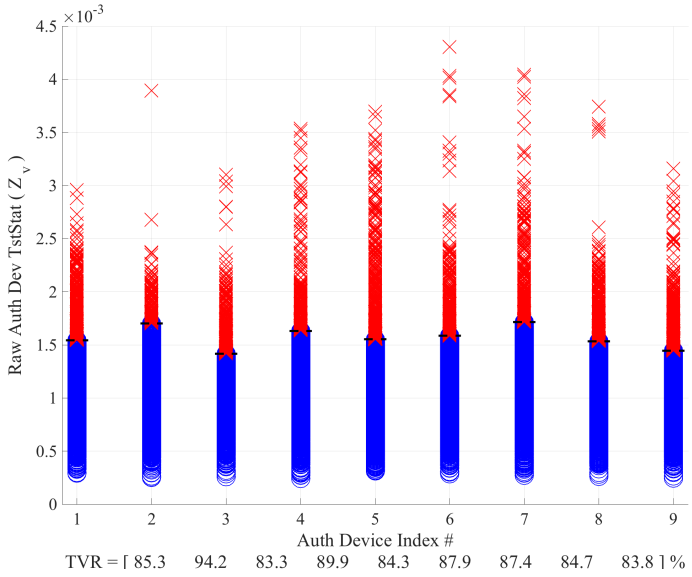

Figure 37. Device ID Verification stem plots for $N_C = 9$ Class Like Model Discrimination (LMD) at SNR_{col} for Case A using Euclidean distance as a measure of similarity. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx 2500$ authorized attempts. Red X's indicate access incorrectly denied and blue circles indicate access correctly granted. The average TVR was approximately 87%.

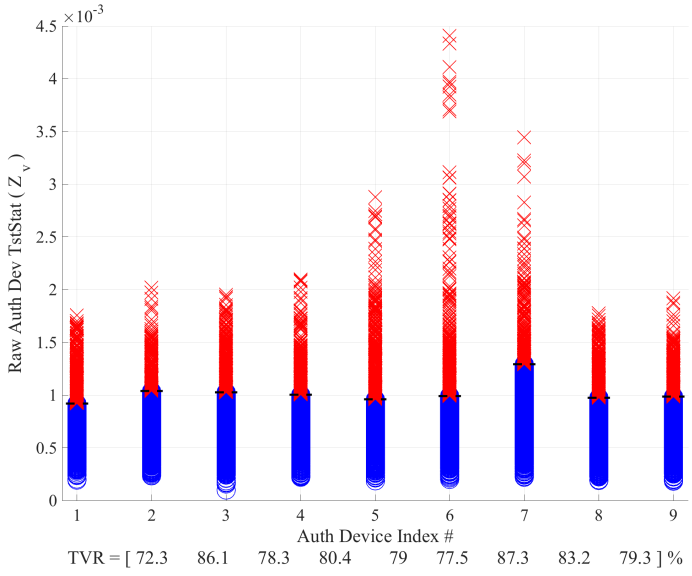

Figure 38. Device ID Verification stem plots for $N_C = 9$ Class Like Model Discrimination (LMD) at SNR_{col} for Case B using Euclidean distance as a measure of similarity. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx 2500$ authorized attempts. Red X's indicate access incorrectly denied and blue circles indicate access correctly granted. The average TVR was approximately 80%.

falsely presenting the credentials of these devices.

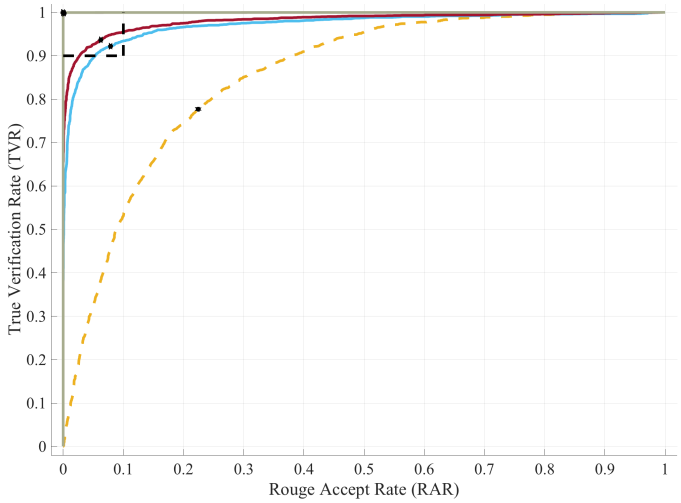

Figure 39. Rogue Device ID Verification ROC curve for $N_C = 9$ Class Like Model Discrimination (LMD) at SNR_{col} for Case A using Device 9 and $N_{rg} = 3$ rogue devices. The black dashed box represents the area where TVR $\geq$ .9 and RAR $\leq$ .1. 8/9 devices were successful for this assessment with the failure (Device 3) denoted by the dashed curve.

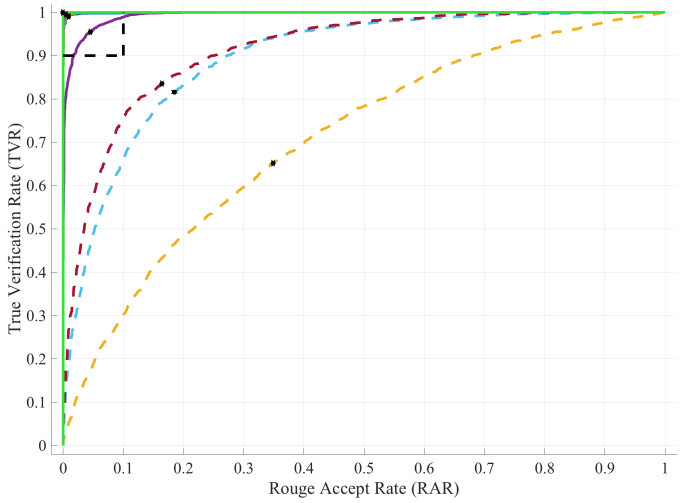

Figure 40. Rogue Device ID Verification ROC curve for $N_C = 9$ Class Like Model Discrimination (LMD) at SNR_{col} for Case B using Device 9 and $N_{rg} = 3$ rogue devices. The black dashed box represents the area where TVR $\geq$ .9 and RAR $\leq$ .1. 6/9 devices were successful for this assessment with failures denoted by dashed curves.

The burst-by-burst grant/deny access assessment for the $N_C = 9$ class LMD verification are presented in Figure 41 and 42. The device dependent EER thresholds for

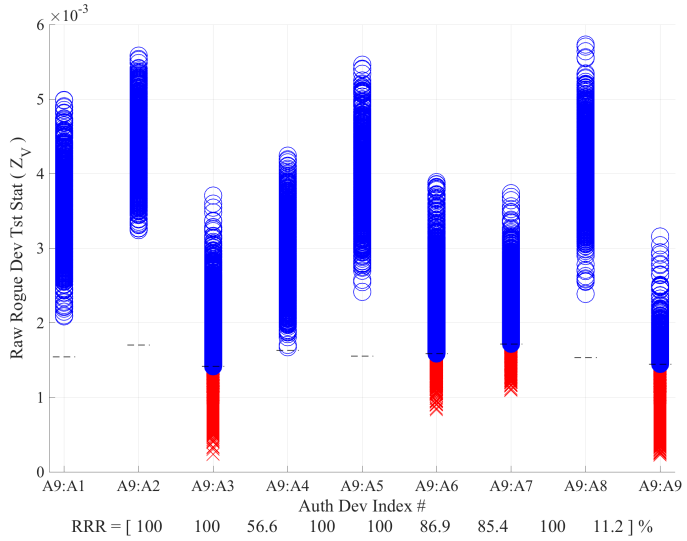

Figure 41. Rogue Device Verification at SNR_{col} for Case A using Device 9 as the rogue device. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx$ 5000 rogue attempts. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied. 5/9 devices had a RRR $\geq$ 90% when Device 9 was falsely presenting credentials.

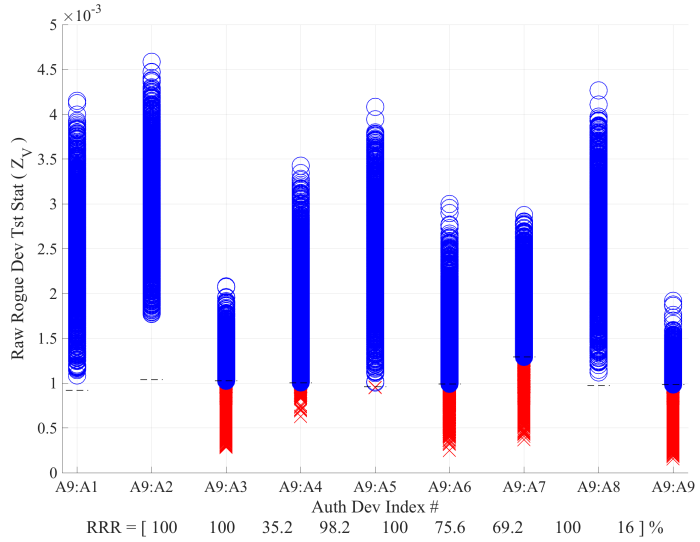

Figure 42. Rogue Device Verification at SNR_{col} for Case B using Device 9 as the rogue device. Results are presented as a burst-by-burst grant/deny access assessment for $N_{test} \approx$ 5000 rogue attempts. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied. 5/9 devices had a RRR $\geq$ 90% when Device 9 was falsely presenting credentials.

these stem plots are displayed as the colored circles on the ROC curves for authorized Device ID verification. As with the $N_C = 4$ class results, the O's represent devices

Table 10. Average Rogue Rejection Rates (%) for all 9 class rogue assessments at each SNR_{Δ}. 27 unauthorized and 64 compromised rogue rejection assessments were completed at each SNR_{Δ}.

	SNR_{Δ}	-44	-39	-34	-29	-24	-19	-14	-9	-4	0
Case A	Compromised	53.20	55.85	56.62	63.33	71.29	83.69	86.63	93.27	94.80	95.57
	Unauthorized	88.89	99.55	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
Case B	Compromised	52.35	52.37	53.02	56.32	67.32	76.54	80.96	85.87	88.59	89.48
	Unauthorized	82.86	94.35	99.95	100.00	100.00	100.00	100.00	100.00	100.00	100.00

correctly denied access and the X's indicate devices that were incorrectly granted access. The dashed horizontal black lines represent the device dependent EER. The average RRR for Case A is $\approx 91\%$ and the average RRR for Case B is $\approx 85\%$. Device 3 is the worst performing device and Rogue (compromised) Device 9 is rejected $\approx$ 100% of the time when falsely presenting Device 1, 2, 4, 5, and 8's credentials for both cases. Rejection rates for Device 3, 6, and 7 decrease by greater than 20% for Case B indicating a higher degree of similarity between devices from fingerprints generated with the shorter ROI.

Consistent with the $N_C = 4$ class CLD problem, all true rogue devices were rejected 100% of the time when presenting any of the nine authorized devices credentials. Stem plots are very similar to the $N_C = 4$ class results for Device 1 and are instead presented here in tabular form in Table 10. Table 10 also presents the average RRR for all rogue assessments at each SNR_{Δ}. On average, unauthorized devices were rejected $\geq 90\%$ of the time even when SNR was degraded by 39 dB.

Results for the $N_C = 9$ class LMD assessment indicate that WS-DNA may not be suitable for identifying compromised devices when ≥ 9 devices of the same make and model are present on the network. Due to the high similarity between Like-Model devices, a compromised (authorized) device was incorrectly accepted $\geq 60\%$ of the time when falsely presenting credentials and $\%C \geq 90\%$ was not achieved using WS-DNA fingerprint generated using Case B parameters.

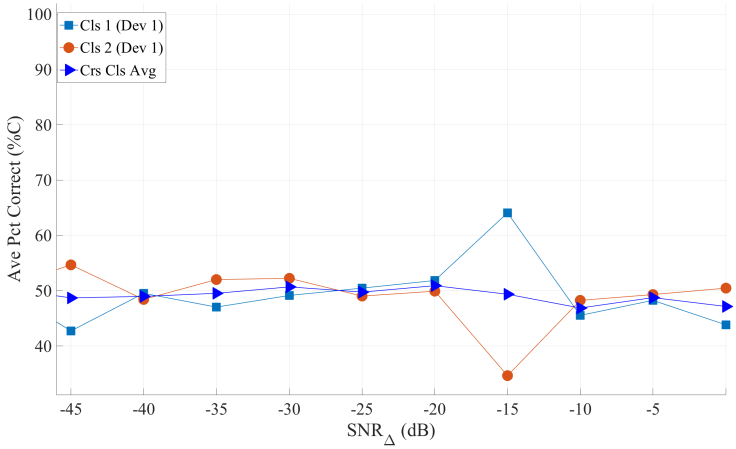

Figure 43. Classification Results for Device 1 compared to itself.

4.4 Thermal Cycling

This section presents the classification results for the CAN transceiver thermal cycling as well as the verification results. All thermal cycling assessments were accomplished using the Case A (entire preamble) ROI. This section begins with a primer for the reader to understand what MDA/ML results typically look like when a device is compared to itself. The intent of MDA/ML is typically to maximize the correct classification and maximize the True Verification Rate (TVR) and the Rogue Rejection Rate (RRR). The intent of the thermal cycling test was to utilize WS-DNA fingerprints and MDA/ML to assess how much a device looks like itself during and after thermal cycling. Success in this case should be defined as minimizing %C to approximately $\frac{1}{N_C}$ as well as minimizing the RRR between classes. In Figure 43, Device 1 was divided into two equal length classes, each composed of interleaved fingerprints. As expected, %C is $\approx 50\%$, or a random guess, for all SNR's. Rogue rejection rates for a device presenting its own credentials can be observed in the $N_C = 4$ class CLD and $N_C = 9$ class LMD assessments and are typically less than 25%.

4.4.1 Classification.

The thermal cycling classification results are presented for two cases. The first case examined is for the $N_C = 6$ class that experienced cold and hot thermal cycling and the second case examined is for the $N_C = 3$ class that only experienced heat cycling as outlined in Section 3.3.

4.4.1.1 6 Class Thermal Cycling.

Each of the $N_C = 6$ classes is composed of bursts collected at different temperatures as outlined in Section 3.3. The classification results are presented in Figure 44. Classification results at SNR_{col} indicate that each class of the CAN transceiver looks

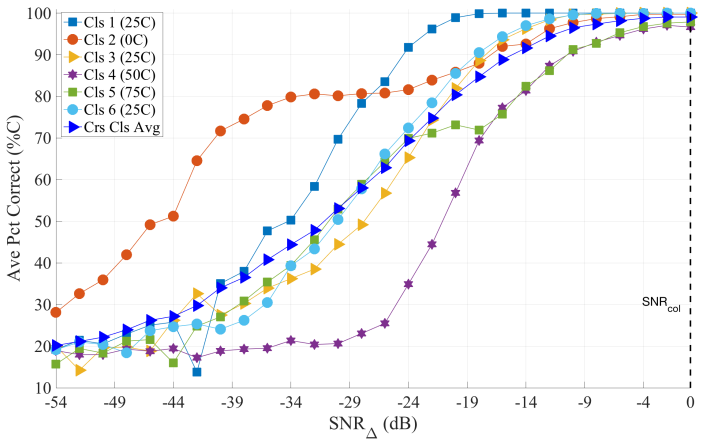

Figure 44. Classification Results for $N_C = 6$ class thermal cycling problem. Each class represents a collection at a different temperature.

Table 11. Confusion Matrix results for $N_C = 6$ Class thermal cycling. Each class represents a collection at a different temperature (or after different thermal cycling).

	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6
Class 1	100	0	0	0	0	0
Class 2	0	99.72	0	0.04	0.24	0
Class 3	0	0	100	0	0	0
Class 4	0.36	0	0	96.16	3.48	0
Class 5	0	0.8	0	2.4	96.8	0
Class 6	0	0	0.04	0	0	99.96

different at different temperatures. Class 2 (freezing) has statistically better classification from $SNR_{\Delta} \geq$ -54 dB SNR_{Δ} = -28 dB and Class 1 (baseline 25 °C) had statistically better classification from $SNR_{\Delta} \geq$ -22 dB to SNR_{Δ} = -14 dB.

The confusion matrix results at SNR_{col} are presented in Table 11. There is almost no confusion between classes at this SNR with most of the confusion occurring between Class 2, 4 and 5. This confusion may be a result of the wire configuration for these collections as all wires were compressed in the refrigerator and oven used for thermal cycling. There was almost no confusion between Class 1, Class 3 and Class 6 (all 25 °C) which may be attributed to environmental or collection bias since only one collection was made per class for this assessment. Results are further assessed for device similarity in the verification process.

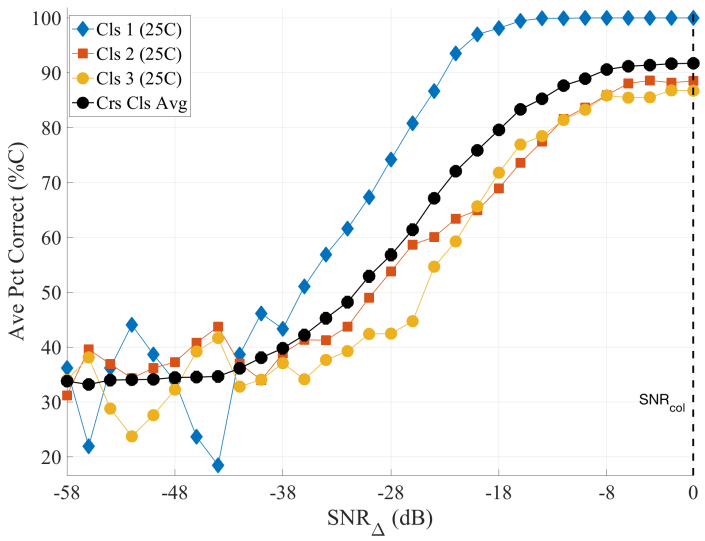

Figure 45. N_C **= 3 class MDA/ML classification results. Each class was collected at ambient temperature.**

Table 12. Confusion Matrix results for N_C **= 3 Class thermal cycling. Each class represents a collection at ambient temperature.**

	Class 1	Class2	Class 3
Class 1	100	0	0
Class 2	0	87.27	12.73
Class 3	0.07	15.29	84.44

4.4.1.2 3 Class Thermal cycling.

$N_C = 3$ Class thermal cycling classification results are presented in Figure 45 and confusion matrix results are presented in Table 12. The purpose of this assessment is to determine "tomorrow" how much this device looks like itself "yesterday and today" after experiencing at least a 25 °C temperature change. The classification results at SNR_{col} indicate that Class 1 looks completely different from Class 2 and 3 as it was correctly classified %C = 100% of the time even though each class was collected at 25 °C. Class 2 and 3 look more similar to each other although %C $\geq$ 80% for both which may result from additional hardware changes as the device continued to cool between collections. These results imply that heat cycling does have an effect on the fingerprints and the device does not look like itself after being heated. Verification results provide an assessment of how similar Class 3 is to Class 1 and 2.

4.4.2 Verification.

Thermal cycling verification results are presented in this section for both the $N_C = 6$ and $N_C = 3$ class assessment. Verification was accomplished to determine how similar each class is before, during, and after thermal cycling.

4.4.2.1 6 Class Thermal Cycling.

Rogue Device ID verification was implemented for two cases for the $N_C = 6$ class problem; Case 1 included Class 6 in the model development and Case 2 excluded Class 6 from model development. Class 6 was used as a rogue class for each case to assess which class it was most similar to. Figure 46 presents the rejection results when Class 6 is included in the model development and Figure 47 presents the results when Class 6 is excluded from model development. The results indicate that Class 6 had the highest similarity to Class 3 with a RRR of 84% when Class 6 is presented as a true rogue class.

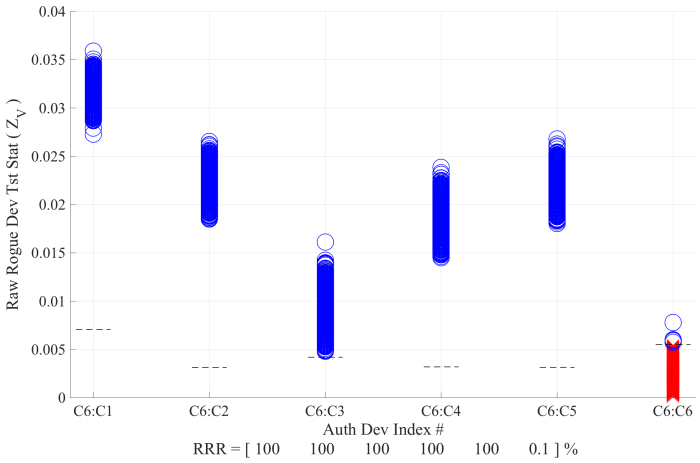

Figure 46. Rogue Device Verification at SNR_{col} for Case A (entire preamble) using Class 6 (included in model development) as the rogue class. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied.

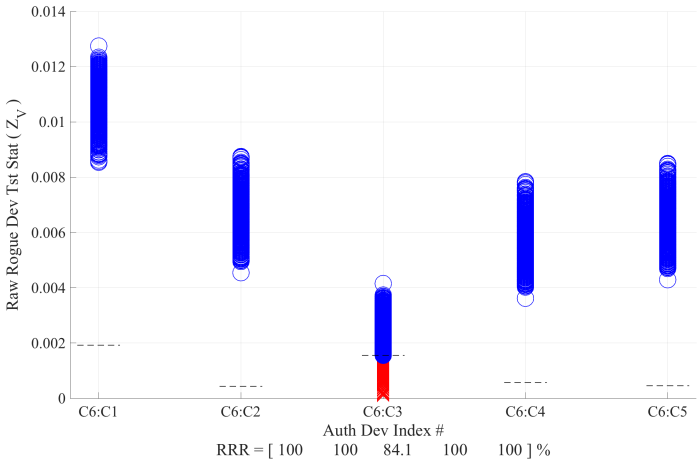

Figure 47. Rogue Device Verification at SNR_{col} for Case A using Class 6 (excluded from model development) as the rogue class. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied.

Class 1, 3, and 6 were all collected at an ambient temperature of approximately 25 °C. Class 3 and 6 may not be similar to Class 1 due to wire configurations during collection or potentially environmental bias. These results coupled with the classification results indicate that fingerprints at different temperatures and after thermal cycling are not similar.

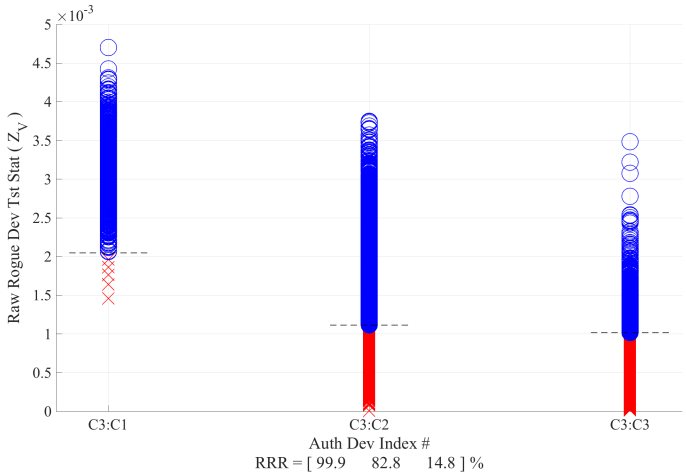

Figure 48. Rogue Device Verification at SNR_{col} for Case A (entire preamble) using Class 3 (included in model development) as the rogue class. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied.

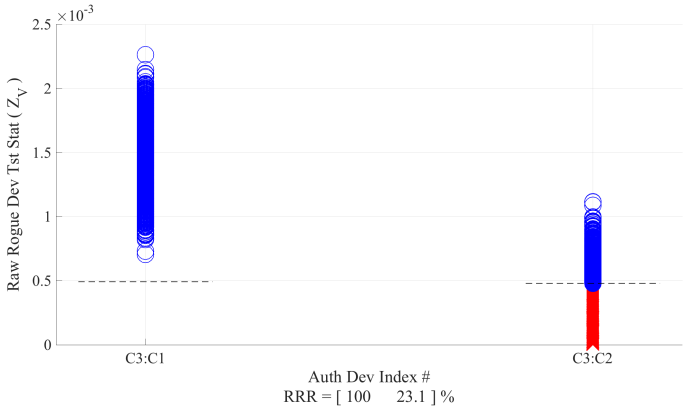

Figure 49. Rogue Device Verification at SNR_{col} for Case A using Class 3 (excluded from model development) as the rogue class. Red X's indicate access incorrectly granted and blue circles indicate access correctly denied. Class 3 has a high similarity to Class 2.

4.4.2.2 3 Class Thermal Cycling.

Rogue rejection results are presented for two cases for the $N_C = 3$ class thermal cycling assessment; in Case 1, Class 3 is included in model development and in Case 2, Class 3 is excluded from model development. All collections for this experiment were taken at approximately 25 °C but Class 2 was collected after the device was heated from ambient temperature to 50 °C and allowed to cool back down to ambient temperature. Class 3 was collected ≈ 24 hours after Class 2 and experienced no thermal

cycling or configuration changes. Results for both cases are presented in Figure 48 and 49 . These results indicate that Class 3 has some similarity to Class 2 and almost no similarity to Class 1. When Class 3 is included in the model development, the RRR is 82.8% when presenting Class 2 credentials. When Class 3 is excluded from model development, only 23% of attempts were rejected indicating a high degree of similarity. The classification and verification results for the $N_C = 3$ class thermal cycling problem indicate that the fingerprints do change when the CAN transceiver is heated and allowed to cool back down. The average correct classification $> 50\%$ for Class 2 and 3 indicate that the device looks different, but a RRR $\leq 25\%$ indicate the classes have some similarity to each other.

4.4.3 3 Class Cross Lot, Cross Temperature.

This section presents the cross class average correct classification for $N_C = 3$ class Cross Lot assessment. All devices were the same part number, two were from the same lot and one was a different lot. All CAN transceivers were thermally cycled and

[2]Class 1 was collected using the same collection methodology presented in Section 3.3. Class 2-4 only consisted of one collection at each temperature and may have been subjected to additional environmental bias.

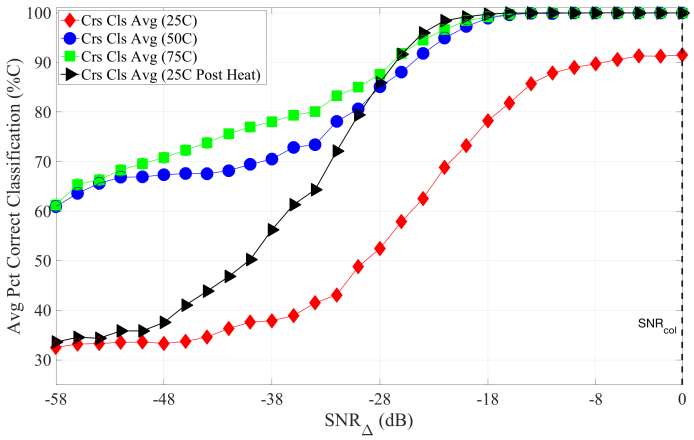

Figure 50. Classification Results for $N_C = 3$ class Cross Lot CAN transceivers across multiple temperatures. %C improves during and after thermal cycling.[2]

correct classification was assessed for 1) baseline 25 °C, 2) 50 °C, 3) 75 °C, and 4) 25 °C after thermal cycling. The results for the cross class average correct classification at all four temperatures are displayed in Figure 50. The maximum %C achieved for the baseline 25 °C collection was $\approx$ 90% at SNR_{col} but there was almost no confusion between the three devices at 50 °C, 75 °C, and at 25 °C once the devices were cooled following thermal cycling. The cross class average results after thermal cycling at 25 °C are statistically better than the baseline 25 °C results at $SNR_{\Delta} \geq$ -48 dB. Classification results at elevated temperatures indicate that devices are even more dissimilar because %C does not reach $1/N_C$, or a random guess, within the same SNR_{Δ} range as the ambient temperature classes. These results may also indicate that although each device does not look like itself at different temperatures as previously shown in Figure 44 and 45, there are still features exclusive to each device that allow for correct classification when presented with fingerprints from another device that also has an elevated temperature. These results are not definitive but warrant further investigation into the effects of temperature on device discrimination.

V. Summary and Conclusions

This chapter provides a summary and conclusion for the results obtained from Wired Signal Distinct Native Attribute (WS-DNA) fingerprint discrimination of Electronic Control Units. A summary of this research and its applications is provided in Section 5.1. This section also provides a summary of device classification and verification for the Cross Lot Discrimination (CLD) and Like Model Discrimination (LMD) and conclusions for the preliminary investigation of temperature effects on fingerprinting and discrimination. Lastly, possible extensions to this research are presented in Section 5.2.

5.1 Research Summary

As automobiles become more connected and autonomous with the use of technologically advanced ECUs, the need for establishing network security becomes more imminent. Hackers have proven that they can incapacitate vehicles by compromising authorized ECUs or by installing rogue devices on the network [13, 20, 31]. Because most vehicles contain electronic controls and embedded systems on a network, this threat is not limited to automobiles but may extend to heavy vehicles, ships, and tanks. This research showed that WS-DNA discrimination is a viable solution for ECU classification and verification. Although development boards like the Ardunio and Beagle Board are able to simulate ECUs, the differences in the transition regions and the amplitudes provide enough information to reject these devices when compared to authorized ECUs. Using only the message preamble of an ECU for $N_C = 4$ class CLD and $N_C = 9$ class LMD, 100% of the rogue attempts to access the network were denied for three different rogue devices. Using a different Steering Angle Sensor as a compromised device resulted in $> 99\%$ rogue rejection for the CLD and $> 95\%$ of

rogue attempts were denied for the LMD problem. Additionally, the average correct classification of the $N_C = 4$ devices was ≥ 90 % at SNR_Δ = -8 dB and %C = 99% was achieved at SNR_{col}. Classification results were lower for the LMD, a maximum %C = 90% was achieved at SNR_{col}. As expected, using only the seven bits as the ROI in Case B, classification and verification performance was statistically worse than Case A. The average correct classification %C was reduced by $\approx 3\%$ at SNR_{col} although the average RRR for compromised devices was approximately the same for the Case B CLD assessment. LMD classification results for Case B failed to achieve %C = 90% but the average compromised device rejection rate was still $\geq 89\%$. Even with decreased overall performance, rogue rejection was still 100% for Case B indicating that WS-DNA is suitable to authenticate base frame format ECUs and results look promising for use with extended frame format ECUs based on the results for Case A.

5.1.1 Thermal Effects.

Results from the thermal cycling indicate that fingerprints do change as devices experience temperature variations. Within the $N_C = 6$ class cross temperature assessment, %C $\approx 100\%$ at SNR_{col}, clearly indicating differences in classes. While $N_C = 3$ class ambient temperature assessment collection accounted for possible environmental and collection bias, average %C $\approx 91\%$ with no misclassification between the baseline Class 1 and Class 2 or Class 3. The confusion between Class 2 and Class 3 indicates some similarity but also may indicate that the device continued to changed as it was cooled down.

Although each device looked different after experiencing thermal cycling, the $N_C = 3$ CAN transceivers assessment achieved %C $\approx 100\%$ at elevated temperatures and once each device cooled back down to ambient temperature.

5.2 Future Work

This section provides some potential future extensions to WS-DNA applications for ECUs on the CAN bus.

5.2.1 Alternate Classifiers.

Alternate classifiers such as Random Forest (RndF) or Generalized Relevance Learning Vector Quantization Improved (GRLVQI) could be used to compare discrimination performance to Multiple Discriminant Analysis Maximum Likelihood (MDA/ML).

5.2.1.1 Dimensionality Reduction.

Both Case A and Case B produced a large amount of features for WS-DNA but these features can be reduced. A thorough dimensional reduction analysis (DRA) study could be used to assess classification performance using reduced feature sets. RndF and GRLVQI can be used to accomplish DRA and compare reduced feature classification performance to MDA/ML classification performance[32, 33]. Additionally, RndF can be used to examine the features created during thermal cycling in order to eliminate the temperature dependent features from each class. Following dimensional reduction, a CMD or LMD assessment could be accomplished to determine if the reduced feature set used to eliminate temperature dependence could also be used to achieve device discrimination.

5.2.2 Additional CAN bus DNA Applications.

WS-DNA can be applied to a wider range of CAN bus and ECU discrimination problems. A different fingerprinting methodology, Slope-Based Frequency Shift Keying (SB-FSK), could provide better device discrimination because additional bits in

transient, or variant, regions could be used to generate fingerprints [27]. Examining ECU discrimination for extended frame format ECUs could be useful and potentially validate the claims for Case A. Additionally, discriminating ECUs with different functions on the same vehicle such as a Steering Angle Sensor, an Engine Control Module, and a telematic control unit could be useful. Lastly, LMD and CMD assessments could be performed using only the CAN-Hi or only the CAN-Lo signals.

5.2.3 ECU Measurement Message Jitter.

Many of the ECUs in automobiles are designed to provide measurements of metrics such as engine RPM, angle of the steering sensor, or temperature. During the SAS burst extraction, it was discovered that the even though all sensors were locked and transmitted the same message, there was some intermittent message jitter, or change, observed in every device. The two older devices had the most observed jitter indicating that this phenomenon may be used for device identification or potentially to identify aging or imminent failure of devices.

Bibliography

1. ——. https://store.arduino.cc/arduino-uno-rev3, 2016.

2. Avatefipour, O., Tayyab, M., Hafeez, A., and Malik, H. Linking Received Packet to the Transmitter Through Physical-Fingerprinting of Controller Area Network. In *Workshop on Information Forensics and Security* (2017), pp. 1–6.

3. Carbino, T. J. *Exploitation of Unintentional Ethernet Cable Emissions Using Constellation Based-Distinct Native Attribute (CB-DNA) Fingerprints to Enhance Network Security.* PhD thesis, Air Force Institute of Technology, 2015.

4. Carbino, T. J., Temple, M. A., and Bihl, T. J. Ethernet card discrimination using unintentional cable emissions and constellation-based fingerprinting. *2015 International Conference on Computing, Networking and Communications, ICNC 2015* (2015), 369–373.

5. Carbino, T. J., Temple, M. A., and Lopez, J. A Comparison of PHY-Based Fingerprinting Methods Used to Enhance Network Access Control. In *IFIP Advances in Information and Communication Technology* (2015), pp. 204–217.

6. Carbino, T. J., Temple, M. A., and Lopez, J. Conditional Constellation Based-Distinct Native Attribute (CB-DNA) Fingerprinting for Network Device Authentication. In *2016 IEEE International Conference on Communications, ICC 2016* (2016), pp. 1–6.

7. Cho, K.-t., and Shin, K. G. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. In *USENIX Security Symposium* (2016), pp. 911–927.

8. Choi, W., Jo, H. J., Woo, S., Chun, J. Y., Park, J., and Lee, D. H. Identifying ECUs through Inimitable Characteristics of Signals in Controller Area Networks. *IEEE Transactions on Vehicular Technology 67*, 6 (2018), 4757–4770.

9. Cobb, W. E., Garcia, E. W., Temple, M. A., Baldwin, R. O., and Kim, Y. C. Physical Layer Identification of Embedded Devices Using RF-DNA Fingerprinting. In *IEEE Military Communications Conference MILCOM* (2010), pp. 2168–2173.

10. Cobb, W. E., Laspe, E. D., Baldwin, R. O., Temple, M. A., and Kim, Y. C. Intrinsic Physical-Layer Authentication of Integrated Circuits. *IEEE Transactions on Information Forensics and Security 7*, 1 (2012), 14–24.

11. Coley, G. BeagleBone Black System Reference Manual - A4. 239.

12. Corrigan, S. Introduction to the Controller Area Network (CAN). Tech. Rep. August 2002, 2002.

13. Currie, R. Developments in Car Hacking, SANS Reading Room, 2015.

14. Currie, R. Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering, SANS Reading Room, 2017.

15. Dadour, I. R., Almanjahie, I., Fowkes, N. D., Keady, G., and Vijayan, K. Temperature variations in a parked vehicle. *Forensic Science International* (2011).

16. Erniotti. CAN Bus frame, https://commons.wikimedia.org/wiki/File:CAN-Bus-frame_in_base_format_without_stuffbits.svg, 2018.

17. Evenchick, E. An Open-Source USB to CAN Adapter, https://canable.io, 2017.

18. Gerdes, R. M., Daniels, T. E., Mina, M., and Russell, S. F. Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach. *14th Proceedings of the Network and Distributed System Security Symposium* (2004), 78.

19. Gerdes, Ryan M; Mina, Mani; Russell, S. F. Physical-Layer Identification of Wired Ethernet Devices. *IEEE Trans on Information Forensics and Security 7 7*, 4 (2012), 1339–1353.

20. Greenberg, A. Hackers Remotely Kill A Jeep On The Highway With Me In It, Wired, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway, 2015.

21. Harmer, P. K., Williams, M. D., and Temple, M. A. Using DE-optimized LFS processing to enhance 4G communication security. In *Proceedings - International Conference on Computer Communications and Networks, ICCCN* (2011), pp. 1–8.

22. Jaynes, M., Dantu, R., Varriale, R., and Evans, N. Automating ECU Identification for Vehicle Security. In *2016 15th IEEE International Conference on Machine Learning and Applications, ICMLA 2016* (2017), pp. 632–635.

23. Klein, R., Temple, M., Mendenhall, M., Reising, D. Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance. In *2009 IEEE International Conference on Communications* (2009), pp. 1–5.

24. Kraus, D., Leitgeb, E., Plank, T., and Löschnigg, M. Replacement of the Controller Area Network (CAN) protocol for future automotive bus system solutions by substitution via optical networks. *International Conference on Transparent Optical Networks 2016-Augus* (2016), 1–8.

25. Lassiter, R. M., Graham, S. R., Carbino, T. J., and Dunlap, S. J. Electronic Control Unit discrimination using Wired Signal Distinct Native Attributes (WS-DNA). In *International Conference on Critical Information Infrastructures Security* (2019), pp. 1–20, Under Review.

26. Lopez, J. *Enhanced Industrial Control System (ICS) and Supervisory Control And Data Acquisition (SCADA) Security for ISA99 Level-0 Using Field Device Wired Signal Distinct Native Attribute (WS-DNA) Fingerprints*. Doctoral dissertation, Air Force Institute of Technology, 2016.

27. Lopez, J., Liefer, N. C., Busho, C. R., and Temple, M. A. Enhancing Critical Infrastructure and Key Resources (CIKR) Level-0 Physical Process Security Using Field Device Distinct Native Attribute Features. *IEEE Transactions on Information Forensics and Security 13*, 5 (2018), 1215–1229.

28. Lukacs, M., Collins, P., and Temple, M. Device Identification Using Active Noise Interrogation and RF-DNA Fingerprinting for Non-Destructive Amplifier Acceptance Testing. In *2016 IEEE 17th Annual Wireless and Microwave Technology Conference, WAMICON 2016* (2016), pp. 2–7.

29. Marchetti, M., and Stabili, D. Anomaly detection of CAN bus messages through analysis of ID sequences. *IEEE Intelligent Vehicles Symposium, Proceedings*, 4 (2017), 1577–1583.

30. Murvay, P., and Groza, B. Source Identification Using Signal Characteristics in Controller Area Networks. *IEEE Signal Processing Letters 21*, 4 (2014), 395–399.

31. Paganini, P. CAN Hacking Tools, 20 USD to hack a car remotely, 2014.

32. Patel, H. J., Temple, M. A., and Baldwin, R. O. Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting. *IEEE Transactions on Reliability 64*, 1 (2015), 221–233.

33. Reising, D. R., Temple, M. A., and Jackson, J. A. Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints. *IEEE Transactions on Information Forensics and Security 10*, 6 (2015), 1180–1192.

34. Reising, D. R., Temple, M. A., and Oxley, M. E. Gabor-based RF-DNA fingerprinting for classifying 802.16e WiMAX Mobile Subscribers. In *2012 International Conference on Computing, Networking and Communications (ICNC)* (2012), pp. 7–13.

35. Ross, B., Carbino, T. J., and Temple, M. A. Simulcasted Power Line Communication Network (SPN) Configuration Validation for Home Automation

Applications Using Wired Signal Distinct Native Attribute (WS-DNA) Fingerprinting. *Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017 3312*, 2017 (2017), 313–322.

36. Ross, B. P., Carbino, T. J., and Stone, S. J. Physical-Layer discrimination of Power Line Communications. In *2017 International Conference on Computing, Networking and Communications, ICNC 2017* (2017), pp. 341–345.

37. Suski II, W. C., Temple, M. A., Mendenhall, M., and Mills, R. Radio frequency fingerprinting commercial communication devices to enhance electronic security. *International Journal of Electronic Security and Digital Forensics 1*, 3 (Jan 2008), 301–322.

38. Texas Instruments. Isolated CAN Transceiver - ISO1050. *Datasheet*, June 2009 (2009), 33.

39. Williams, M. D., Munns, S. A., Temple, M. A., and Mendenhall, M. J. RF-DNA Fingerprinting for Airport WiMax Communications Security. In *2010 4th International Conference on Network and System Security, NSS 2010* (2010), pp. 32–39.

40. Williams, M. D., Temple, M. A., and Reising, D. R. Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting. In *GLOBECOM - IEEE Global Telecommunications Conference* (2010), pp. 1–6.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
03–21–2019	Master's Thesis	Sept 2017 — Mar 2019

4. TITLE AND SUBTITLE

Physical Layer Discrimination of Electronic Control Units Using Wired Signal Distinct Native Attribute (WS-DNA) Fingerprints

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Rahn M. Lassiter, Capt, USAF

5d. PROJECT NUMBER

18G230

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-19-M-038

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
2241 Avionics Circle
WPAFB OH 45433-7765
Attn: Steven Stokes
COMM 9375288035
Email: steven.stokes@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYWA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Controller Area Network (CAN) bus is a communication system used in automobiles to connect the electronic components required for critical vehicle operations. These components are called Electronic Control Units (ECU) and each one exercises one or more functions within the vehicle. ECUs can provide autonomous safety features and increased comfort to drivers but these advancements may come at the expense of vehicle security. Researchers have shown that the CAN bus can be hacked by compromising authorized ECUs or by physically connecting unauthorized devices to the bus. Physical layer (PHY) device fingerprinting has emerged as one of the accepted approaches to establishing vehicle security. This paper uses a fingerprinting method called Wired Signal Distinct Native Attribute (WS-DNA) and classification algorithm called Multiple Discriminant Analysis Maximum Likelihood (MDA/ML) to achieve ECU discrimination which includes device classification and verification.

15. SUBJECT TERMS

Device Discrimination, Distinct Native Attribute

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Scott R. Graham, AFIT/ENG
U	U	U	UU	94	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4581; scott.graham@afit.edu